TECHNOLOGY PARTNER PROGRAM

1. Deployment of Palo Alto Networks VM-Series Next-Generation Firewall with Nutanix Calm
2. Applying Microsegmentation with Nutanix Flow and Palo Alto Networks VM-Series

Author: Nutanix and Palo Alto Networks

Contents

Partner Information 4

Use cases for integration into Palo Alto Networks Next-Generation Security Operating Platform 4

Use Case No. 1: Micro-Segmentation 4

Use Case No. 2: Virtual Desktop Infrastructure 4

Palo Alto Networks Products for Integration 4

Integration Benefits 5

Integration Diagram 6

Palo Alto Networks Configuration 6

- Bootstrap ISO 6
- Generate VM-Auth-Code 6
- Bootstrap ISO Image Creation 7
- Create ISO Image 8
- Register the VM-Series Firewall with Auth Codes 9
- Download VM-Series KVM Base Image 10
- Create Panorama Admin Account for Nutanix Calm 10

Partner Product Configuration 13

- Upload VM-Series Image and Bootstrap ISO Image 13
- Create a Project 16
- Import and Configure Calm Blueprint 19
- Deploy Palo Alto Networks VM-Series Application from Calm Blueprint 37
- Verify PAN-OS XML API Configuration Settings 42
- Verify VM-Series Virtual Machines Provisioning 43
- Apply Microsegmentation Policy via Nutanix Flow and VM-Series 45
- Deploy Additional VM-Series via Calm Scale Out 51

Troubleshooting Resources & Documentation 54

- Nutanix 54
- Palo Alto Networks 54

Technical Details 55

- Nutanix 55
- Palo Alto Networks 56

Partner Information

Partner information	
Date	September 27, 2019
Partner Name	Nutanix and Palo Alto Networks
Web Site	https://www.nutanix.com & https://www.paloaltonetworks.com
Product Name	Nutanix Calm & Flow, Palo Alto Networks Panorama & VM-Series
Partner Contact	alliances@nutanix.com; nutanix@paloaltonetworks.com
Support Contact	https://www.nutanix.com/support-services/product-support
Product Description	Automated deployment of Palo Alto Networks VM-Series Next-Generation Firewall and Microsegmentation

Use cases for integration into Palo Alto Networks Next-Generation Security Operating Platform

Use Case No. 1: Micro-Segmentation

- **Challenge:** Virtual applications running on the same host are difficult to selectively segment without complex network design and configuration, often requiring hairpinning traffic and negatively impacting performance. This may lead to increased threat exposure or vulnerabilities in your virtualized environments.
- **Answer:** Micro-segmentation helps reduce the attack surface by preventing lateral movement across your east-west traffic. This is accomplished by deploying VM-Series integrated with Nutanix Flow. Use the Nutanix Calm blueprint to create service chains and deploy VM-Series on every AHV host. With Nutanix Flow, specific traffic can be transparently directed to the VM-Series firewall in the service chain for deep packet inspection based on the user-defined Nutanix Flow policy.

Use Case No. 2: Virtual Desktop Infrastructure

- **Challenge:** Virtual desktops are growing in popularity, but hosting all of these desktops within your core data center also dramatically increases your attack surface without the proper protections in place. The dynamic nature of these desktops can also make security management challenging.
- **Answer:** To address this concern, Nutanix Flow can isolate groups of virtual desktops with a simple security policy and work with VM-Series on AHV to inspect and enforce Layer 7 controls as well as block threats across the virtual desktop infrastructure.

Palo Alto Networks Products for Integration

- Panorama (8.1 & 9.0)
- PAN-OS for VM-Series KVM Image (8.1 & 9.0)

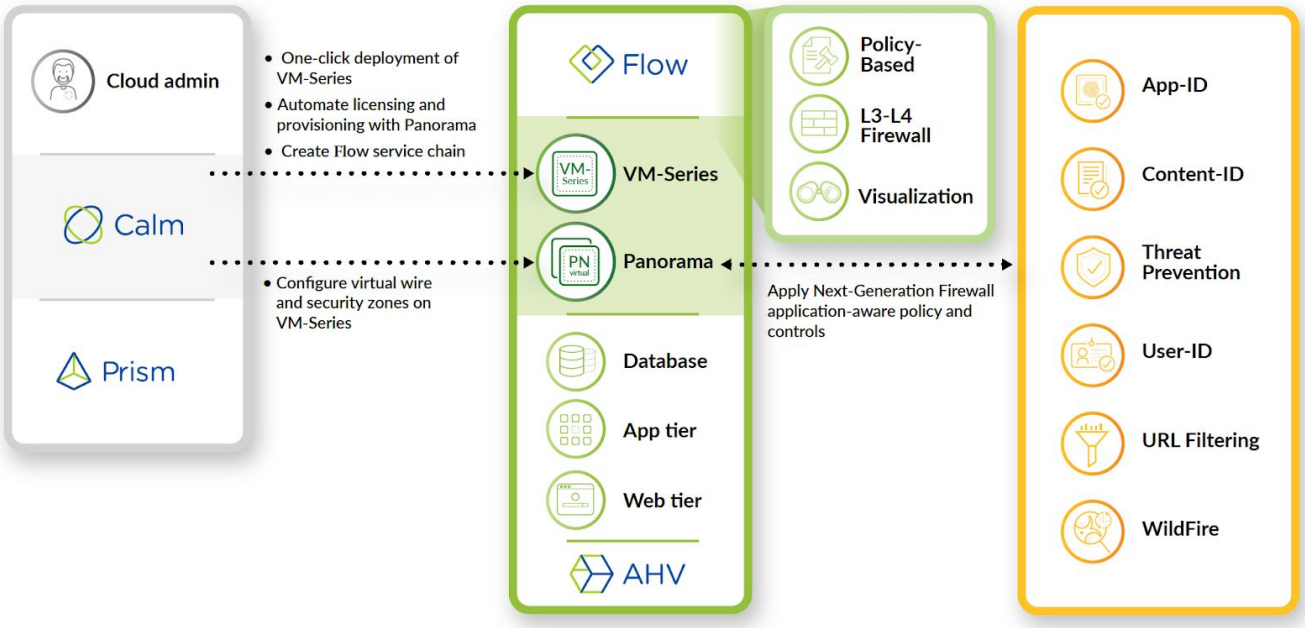
Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Nutanix Versions
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW			
Panorama		PAN-OS 8.1 & PAN-OS 9.0	Prism Central 5.10.6 AOS 5.10.6 with AHV Calm 2.7.0 -or- Prism Central 5.11 AOS 5.11 with AHV Calm 2.7.1
Prisma Access			
Prisma Cloud			
Prisma SaaS			
Traps			
VM-Series		8.1 & 9.0	Prism Central 5.10.6 AOS 5.10.6 with AHV Calm 2.7.0 -or- Prism Central 5.11 AOS 5.11 with AHV Calm 2.7.1
WildFire			
Other			

Integration Benefits

When integrated with Palo Alto Networks VM-Series next-generation virtual firewalls, Flow's ability to control traffic is augmented with industry-leading threat prevention capabilities. While micro-segmentation can help reduce the attack surface of a Nutanix environment, VM-Series threat prevention services ensure that threats attempting to penetrate the perimeter, move laterally across legitimate network connections, or exfiltrate data are detected and stopped. Real-time threat intelligence feeds arm VM-Series with the latest threat signatures

detected across the entire Palo Alto Networks install-base to protect Nutanix environments from the latest zero-day threats.

Integration Diagram



Palo Alto Networks Configuration

Bootstrap ISO

To provide a zero-touch configuration of the Next-Generation Firewall VM-Series instances, which includes automatic licensing and subscription to a Panorama centralized management server, the Bootstrap ISO image provides the configuration elements necessary.

The contents of the Bootstrap ISO image consist of four directories off the root of the ISO filesystem – within two of the four directories are files containing the requisite configuration data. While other configuration elements are possible, they are outside the scope of this guide and are not required for deploying VM-Series with Nutanix Calm.

Generate VM-Auth-Code

Prior to creating the Bootstrap ISO image, you must first generate the VM-Auth-Code. Log into Panorama via the command-line interface (CLI), and issue the following command:

```
request bootstrap vm-auth-key generate lifetime <1-8760>
```

For example, to generate a key that is valid for 24 hours, enter the following:

```
request bootstrap vm-auth-key generate lifetime 24
VM auth key 755036225328715 generated. Expires at: 2019/12/29 12:03:52
```

Bootstrap ISO Image Creation

Create a new folder called *bootstrap* on your computer. Within that folder, create four folders as follows:

config

- *init-cfg.txt* (case-sensitive text file)

content

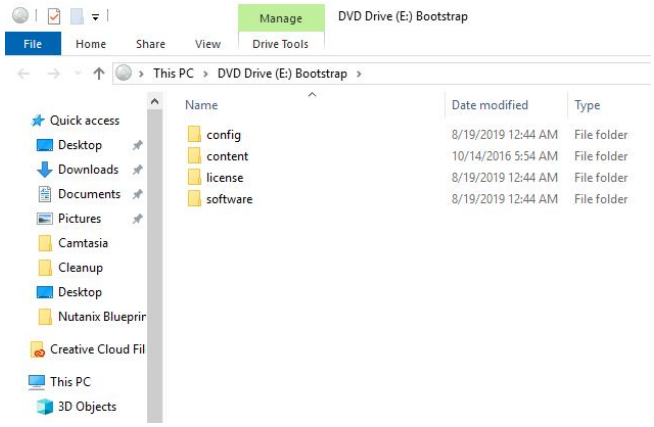
- *Empty*

license

- *authcodes* (case-sensitive text file with no file extension)

software

- *Empty*

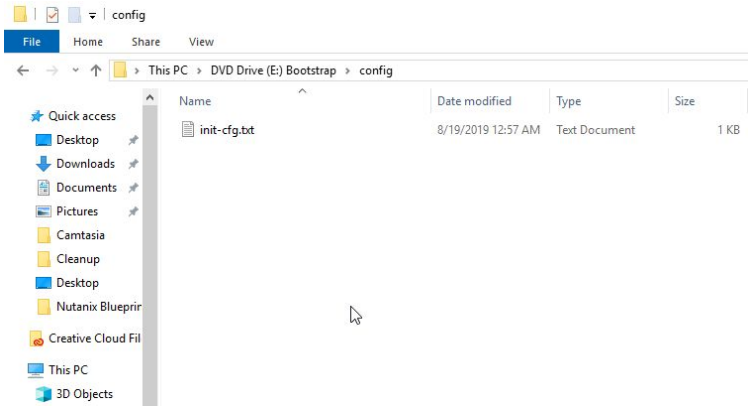


Use a text editor to create the init-cfg.txt and authcodes text files listed above and place them in their respective directory:

init-cfg.txt

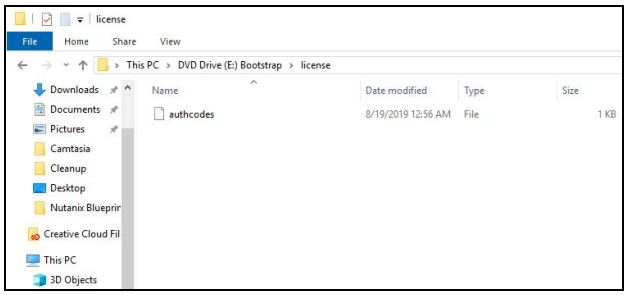
```
type=dhcp-client
op-cmd-dpdk-pkt-io=off
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=
```

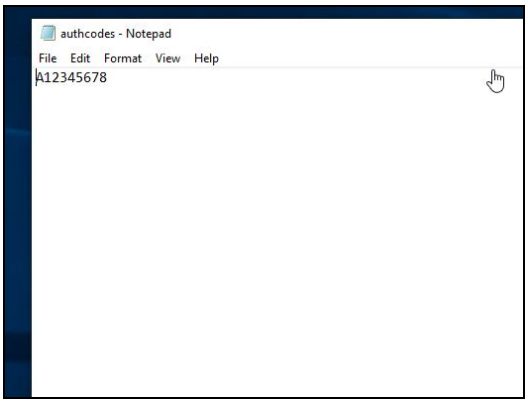
```
vm-auth-key=VM AUTH KEY VALUE
panorama-server=IP ADDRESS OF PANORAMA SERVER
panorama-server-2=
tplname=
dgname=
dns-primary=IP ADDRESS OF PRIMARY DNS
dns-secondary=IP ADDRESS OF SECONDARY DNS
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=no
dhcp-send-client-id=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```



authcodes

A123456789 *enter the value for the auth code as provided by Palo Alto Networks*

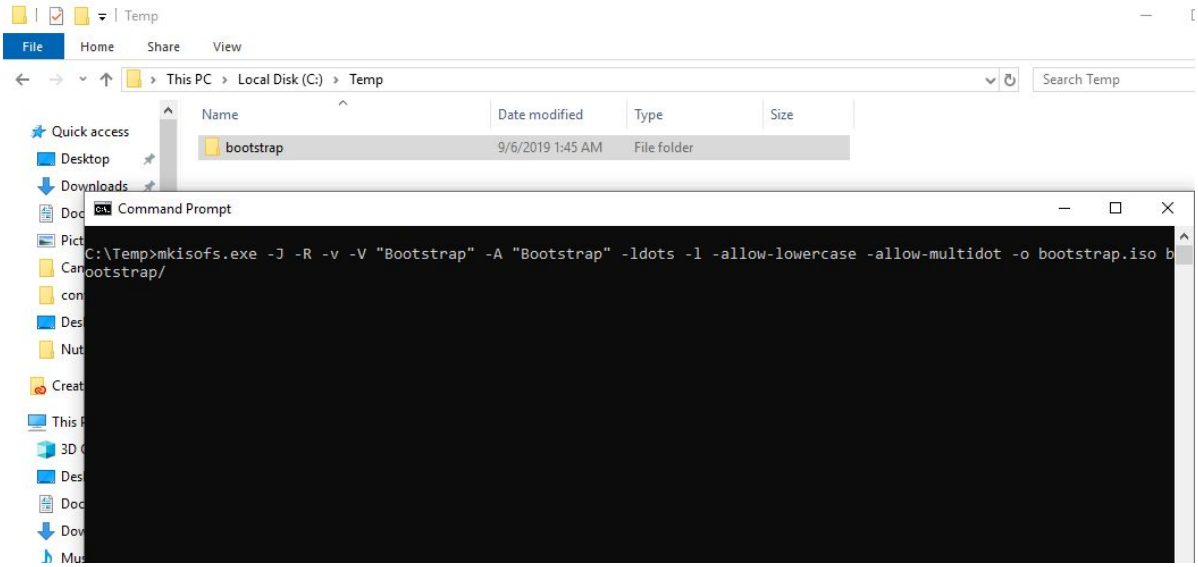




Create ISO Image

Use the 'mkisofs' utility to create the ISO image containing the files and corresponding directory structure above:

```
mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -allow-lowercase -allow-multidot -o
      bootstrap.iso bootstrap/
```



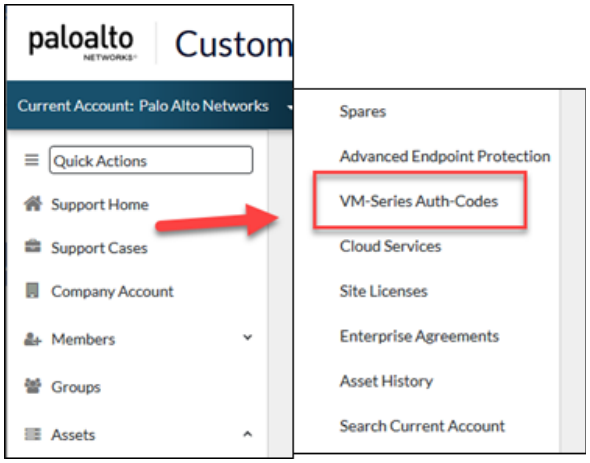
Register the VM-Series Firewall with Auth Codes

Prior to deployment of VM-Series, your auth codes must be activated on the Palo Alto Networks support site otherwise, the automated licensing process will not complete successfully.

Using your web browser, go to:

https://support.paloaltonetworks.com

Navigate to Assets -> VM-Series Auth Codes



Follow the instructions as documented on the Palo Alto Networks TechDocs site to register the auth codes:

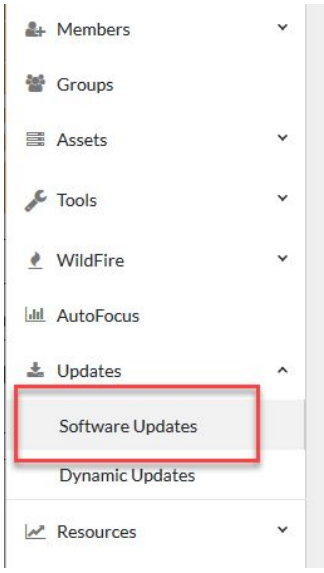
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/license-the-vm-series-firewall/register-the-vm-series-firewall/register-the-vm-series-firewall-with-auth-code.html

Download VM-Series KVM Base Image

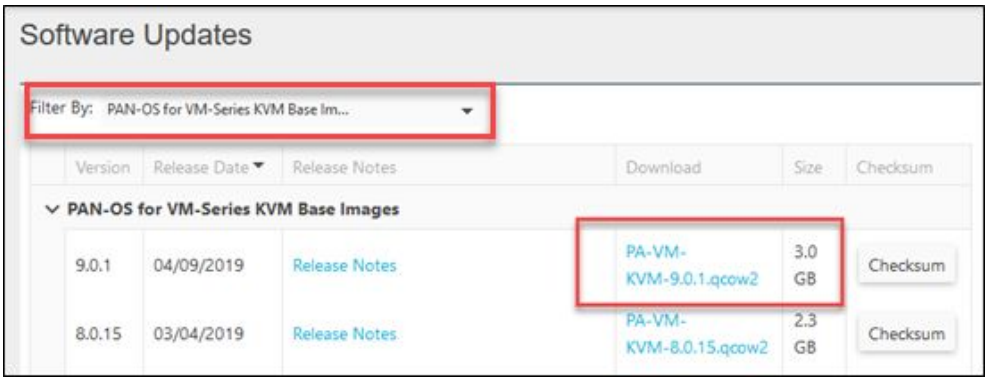
To deploy VM-Series on your Nutanix cluster, download the VM-Series KVM Base Image from the Palo Alto Networks Support Site:

https://support.paloaltonetworks.com

1. Navigate to Assets -> Software Updates



2. In the Filter By drop-down select PAN-OS for VM-Series KVM Base Images
3. Download the most recent version by selecting the link containing the filename as denoted below.

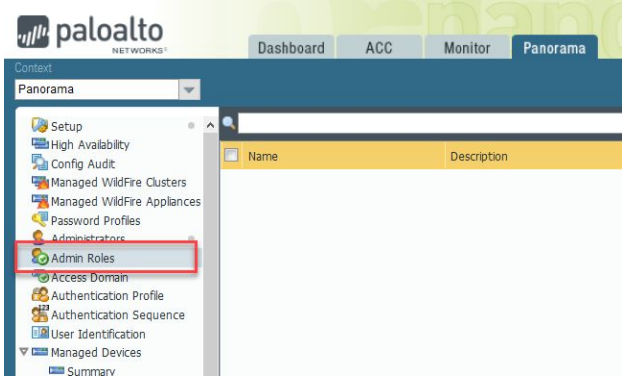


Create Panorama Admin Account for Nutanix Calm

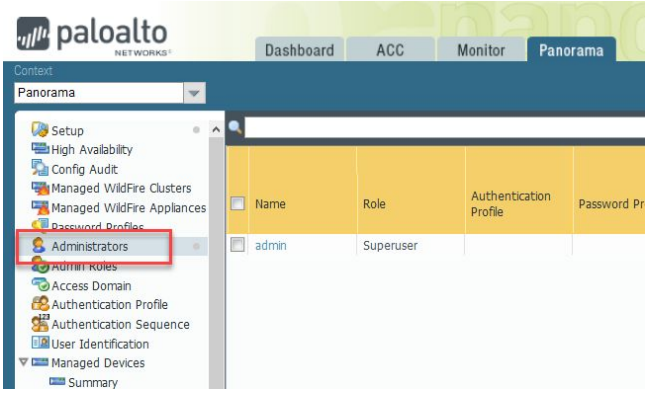
Not only does the Nutanix Calm Blueprint for VM-Series deploy instances across your Nutanix AHV cluster, it also leverages the PAN-OS XML API to automate the configuration of several key elements within Panorama. While it is possible to use an administrative account with Super User privileges, the principle of least-privilege dictates that you should always use administrative accounts with only the permissions necessary to carry out the required functions.

This is easily accomplished through the creation of an Admin Role and Administrator account in Panorama.

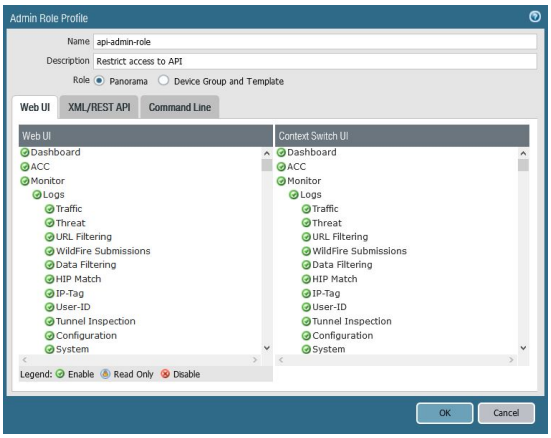
1. Log into the Panorama admin UI and navigate to the *Panorama* tab, then select *Admin Roles*

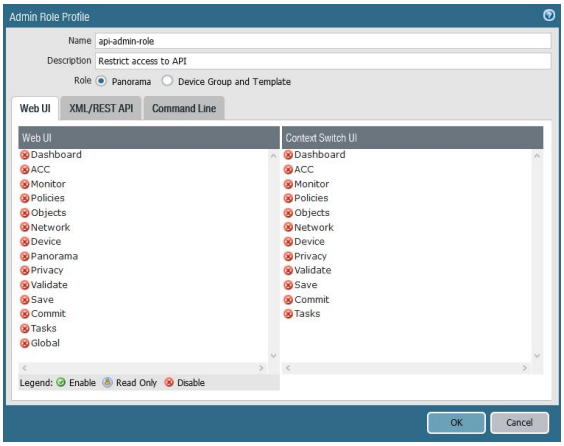


2. Create a new *Admin Role* by clicking *Add* at the bottom of the page (*api-admin-role*)

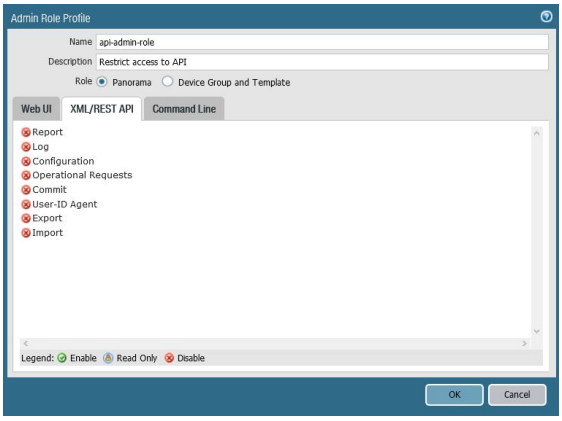


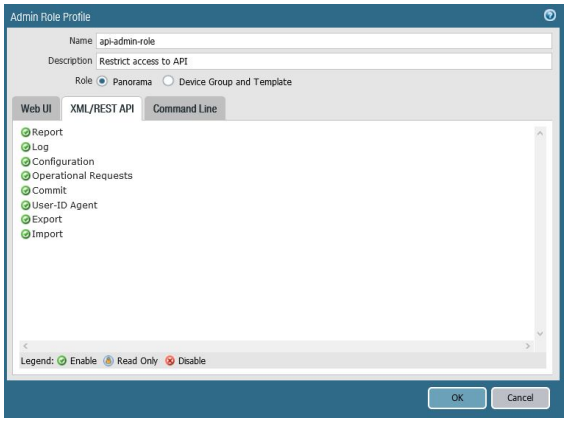
3. Deselect every option on the Web UI tab by clicking on each green checkmark. They will change to red Xs as you proceed through the list



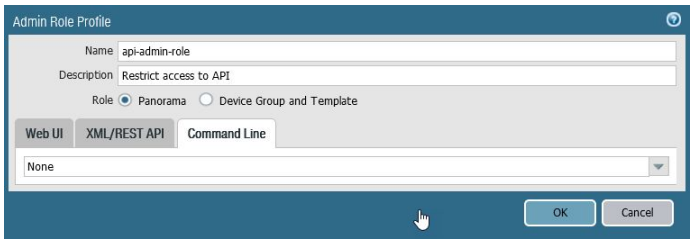


4. Change to the *XML/REST API* tab and repeat the process, this time changing every red X to a green checkmark



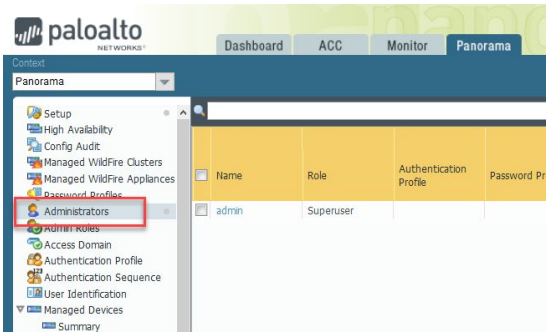


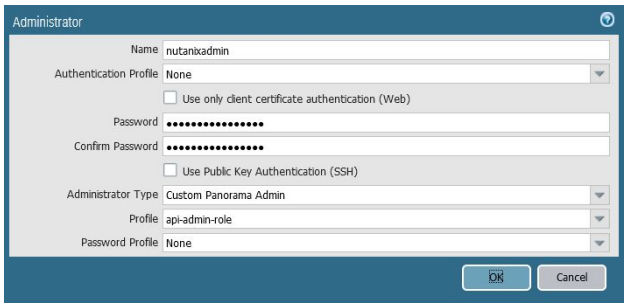
5. No changes are necessary on the *Command Line* tab as no permissions are granted by default



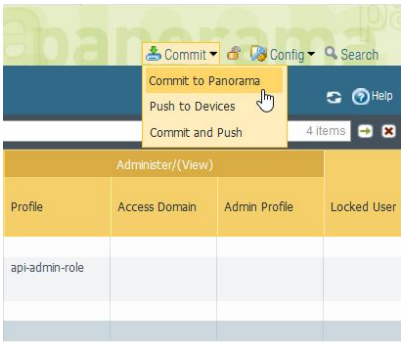
6. Click *OK* to save the changes

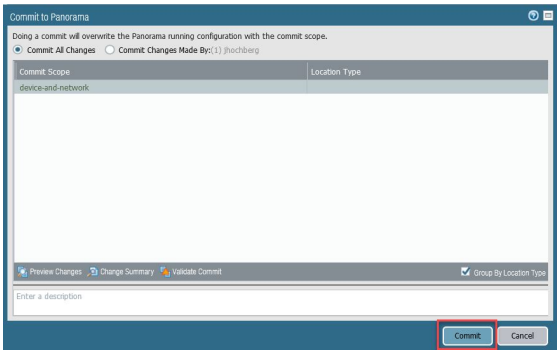
7. Select the *Administrators* menu, then click *Add* to create a new account – provide a username (*nutanixadmin*) and password and confirm the password. Change the *Administrator Type* drop-down select from *Dynamic* to *Custom Panorama Admin*, then select the newly created role in the next drop-down select





8. Click OK to save the new account. Select *Commit -> Commit to Panorama* then click the *Commit* button to apply the newly defined role and account

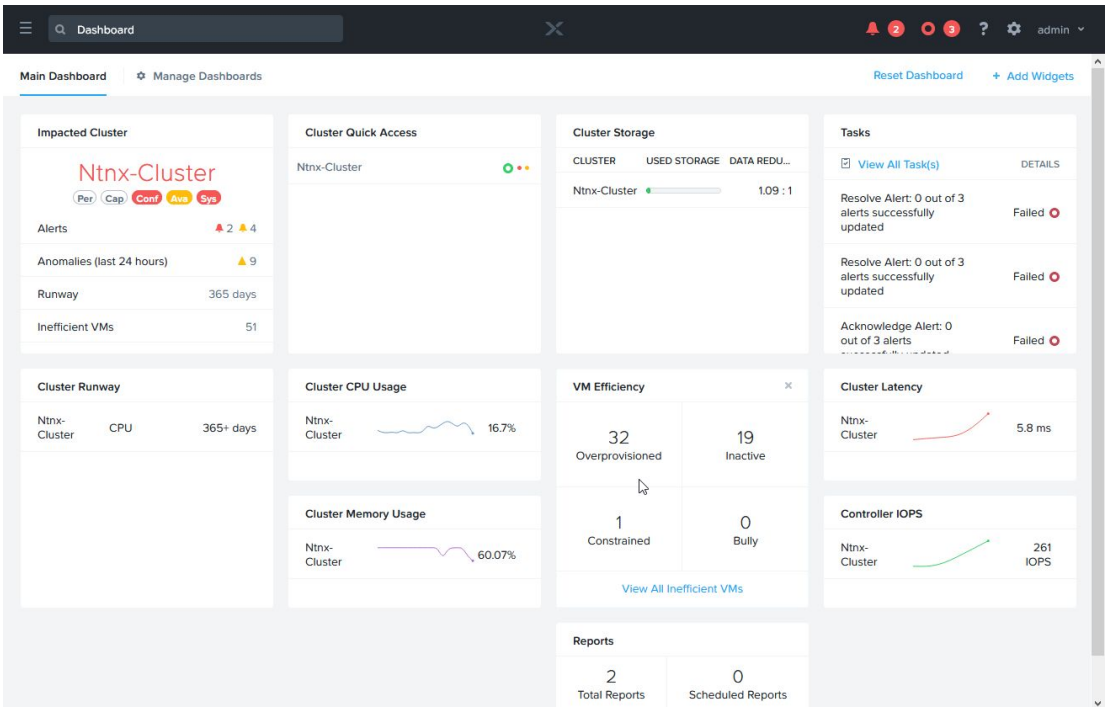




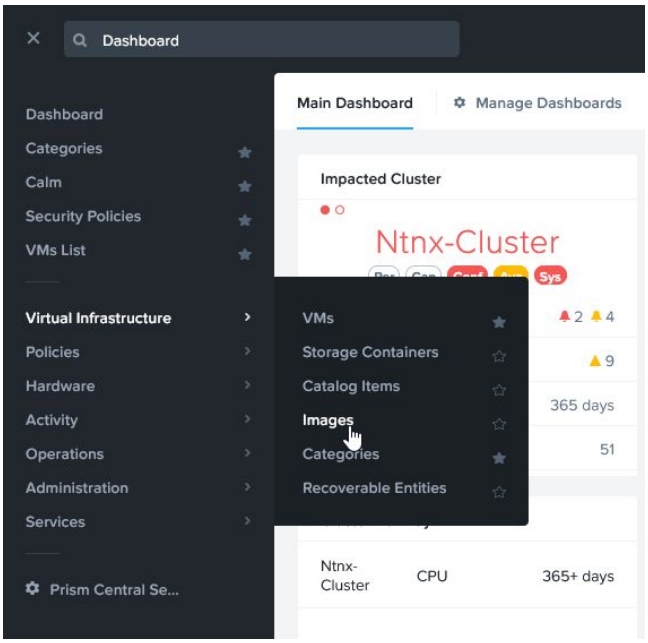
Partner Product Configuration

Upload VM-Series Image and Bootstrap ISO Image

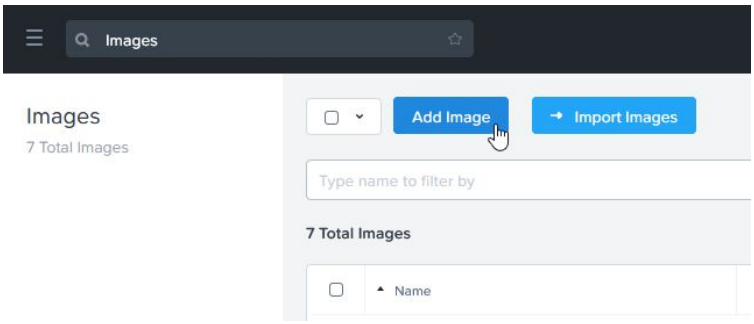
Begin the deployment process by uploading the *PAN-OS for VM-Series KVM Base Image* and *Bootstrap ISO* to Prism Central.



1. From the Prism Central menu, navigate to *Virtual Infrastructure -> Images*

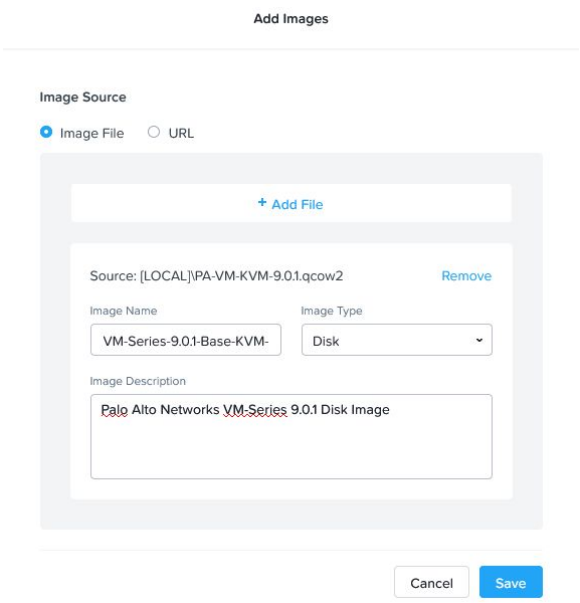


2. Click *Add Image*



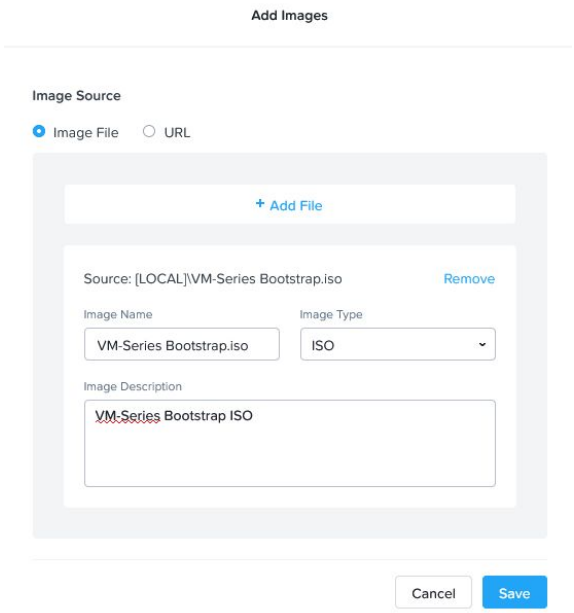
3. Click *+Add File* and browse to the *PAN-OS for VM-Series KVM Base Image*, then click *OK*

4. Input a name in the *Image Name* field or accept the default value, a description (optional), leave the *Image Type* set to *Disk*, and click *Save*



5. Click *Add Image*

6. Click *+Add File* and browse to the *Bootstrap ISO*, then click *OK*

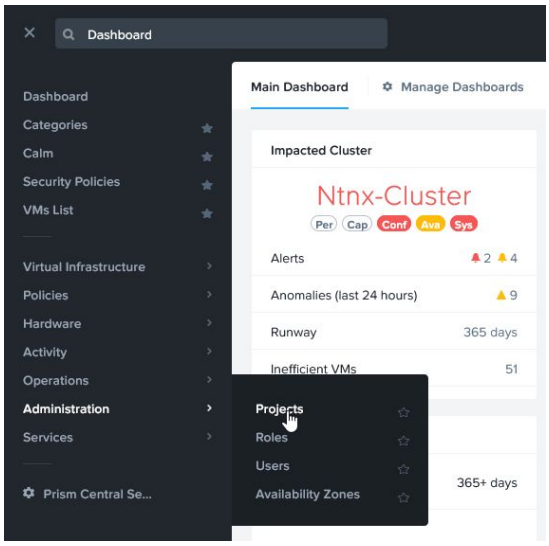


7. Input a name in the *Image Name* field or accept the default value, provide a description (optional), choose *ISO* from the *Image Type* drop-down select, and click *Save*

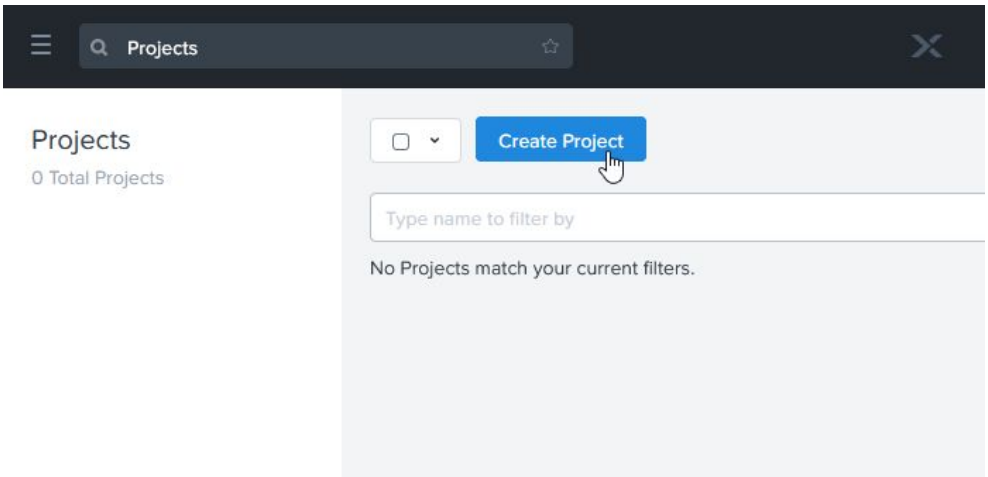
Create a Project

If you already have an existing Nutanix Project defined, that can be used to deploy the Calm Blueprint in lieu of creating a new project. Otherwise, follow the steps in this section to create a new Nutanix Project.

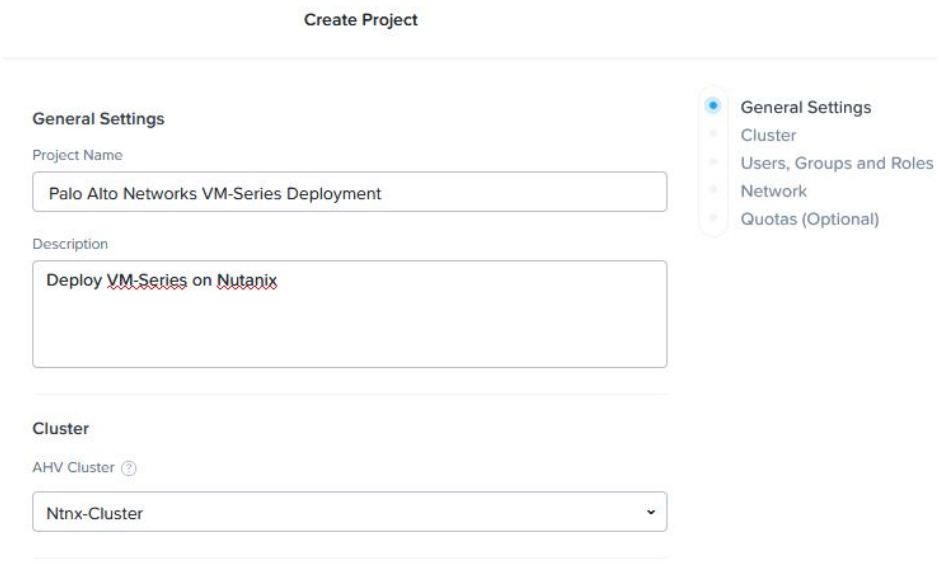
1. Navigate to *Administration -> Projects*



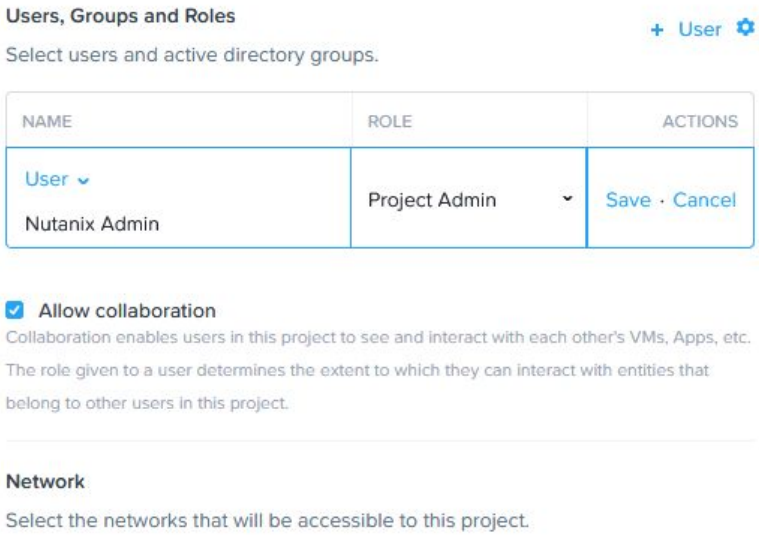
2. Click *Create Project*



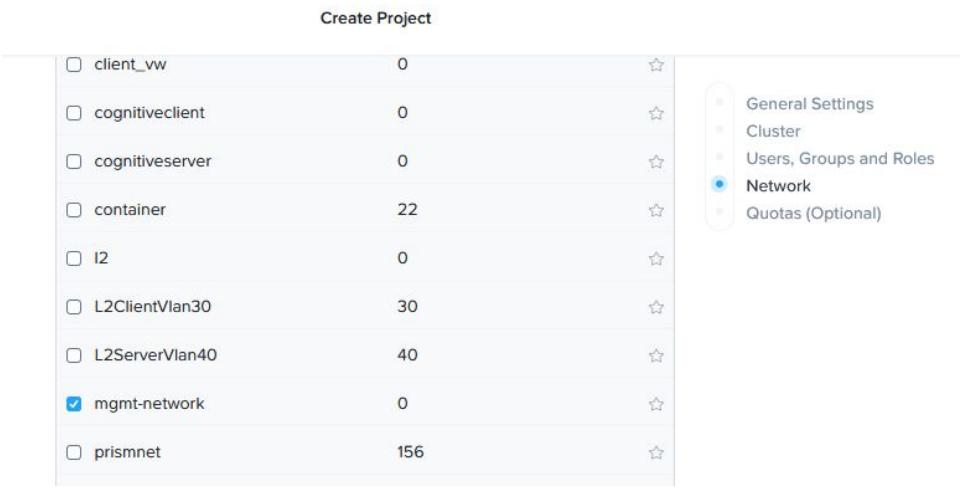
3. Provide a *Name* and *Description*, then choose the *AHV Cluster* on which you want to deploy the VM-Series instances



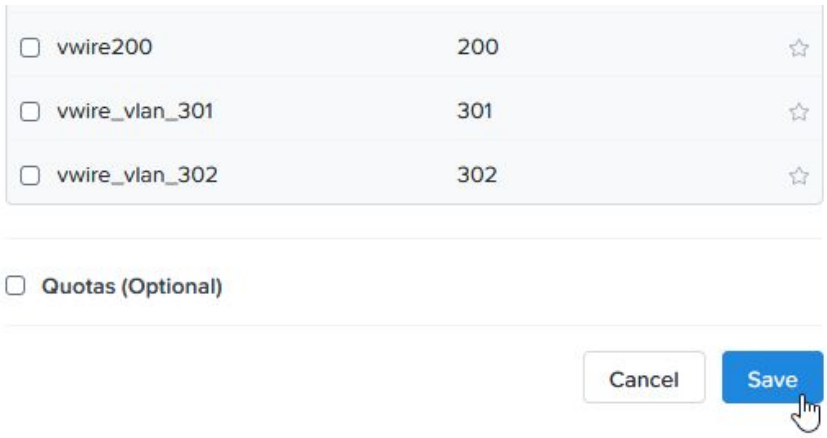
4. Click the *+Users* button then select either *User* or *User Group* in the drop-down select – type in the first few letters of the desired *User* or *User Group* and auto-complete will provide a list of options to select and choose the *Project Admin* role, then click *Save*



5. Select the checkbox next to the *Network* to associate with the Management interface on each VM-Series instance

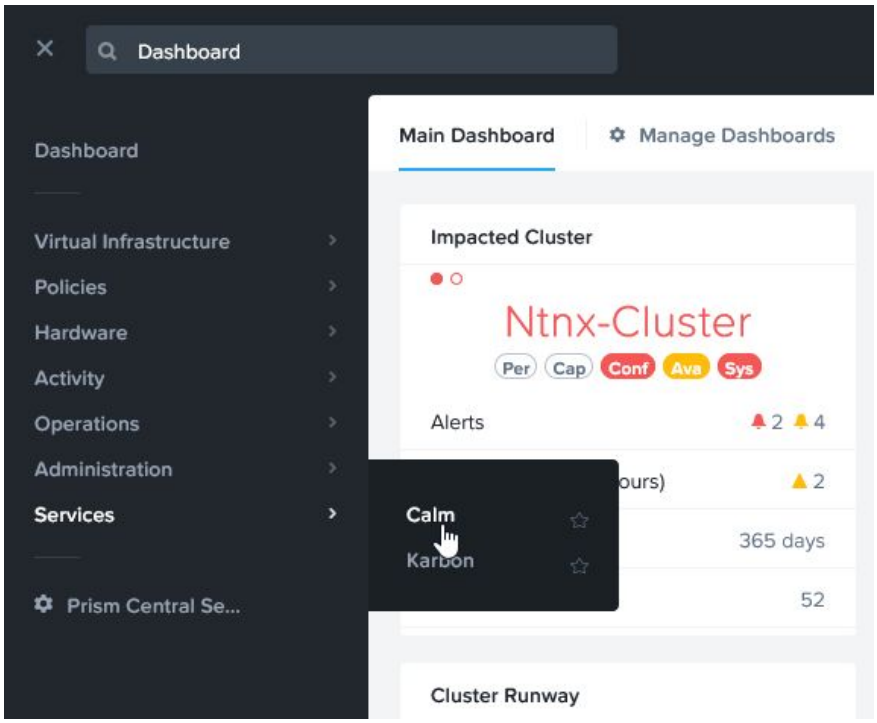


6. Scroll down and click *Save* to finish configuring the *Project*

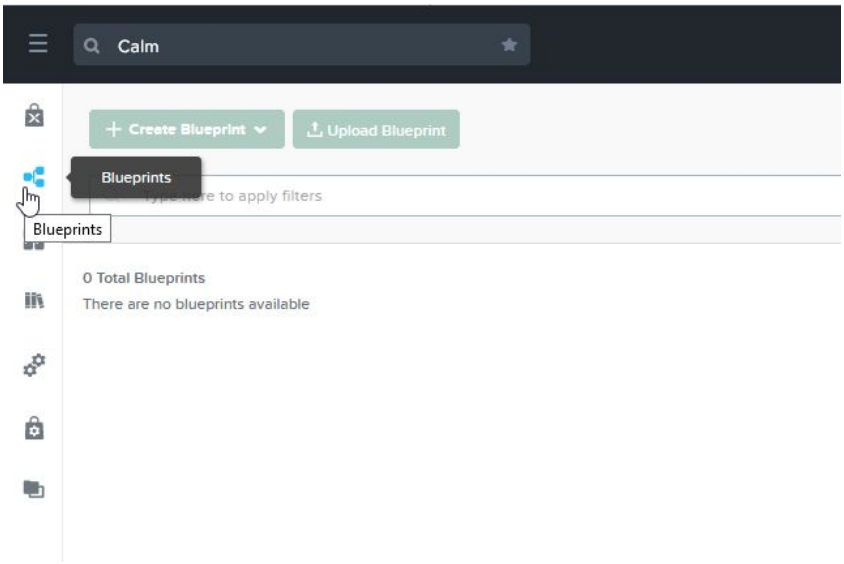


Import and Configure Calm Blueprint

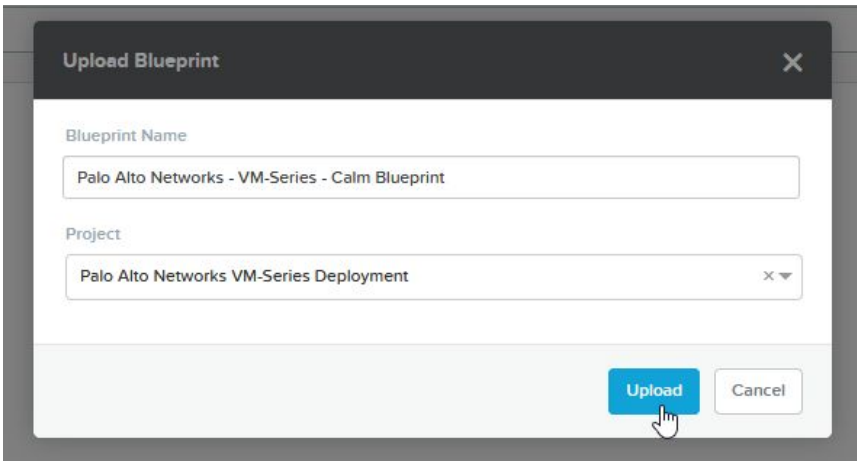
1. Navigate to *Services -> Calm*



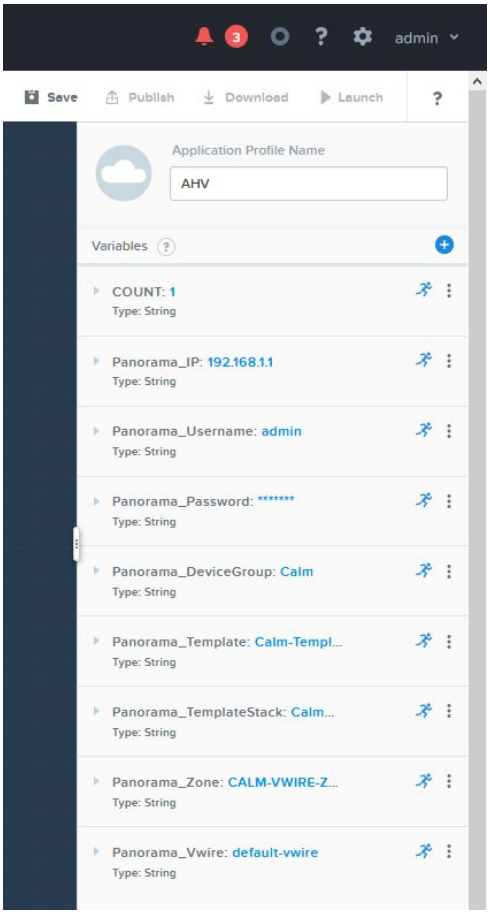
2. Choose the *Blueprints* menu and click on *Upload Blueprint*



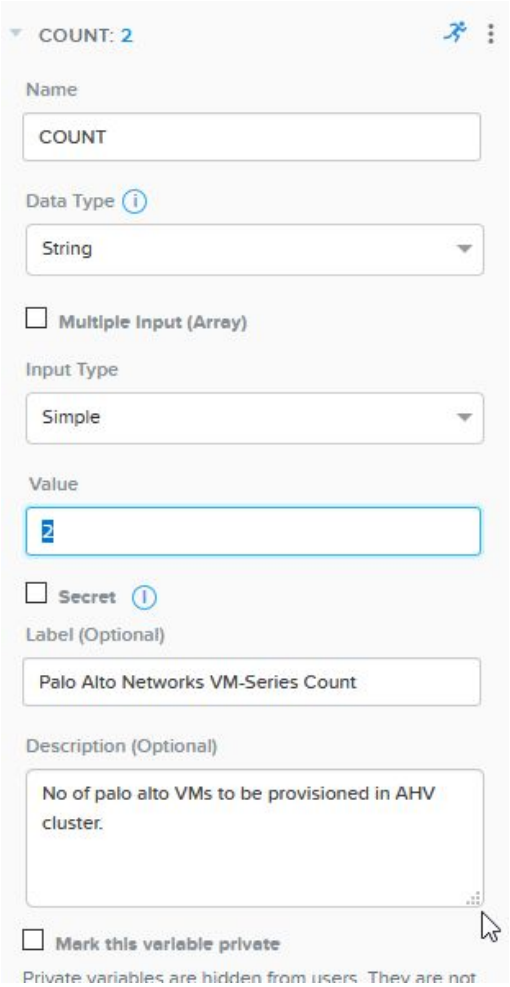
3. Browse to the *Calm Blueprint JSON* file and select the *Project* created in the last section and click *Upload*



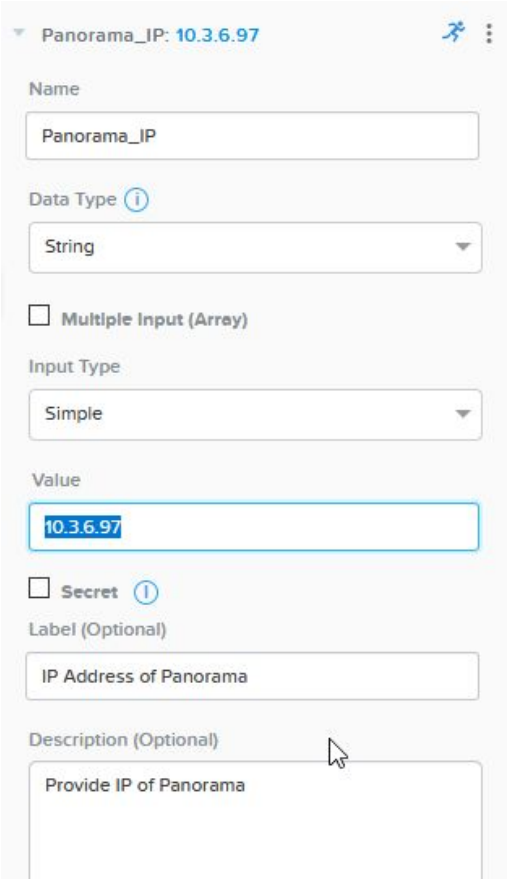
***NOTE**: As you proceed through the remaining steps, ensure you only modify the settings in the Value fields – do not modify any text in the Name fields*



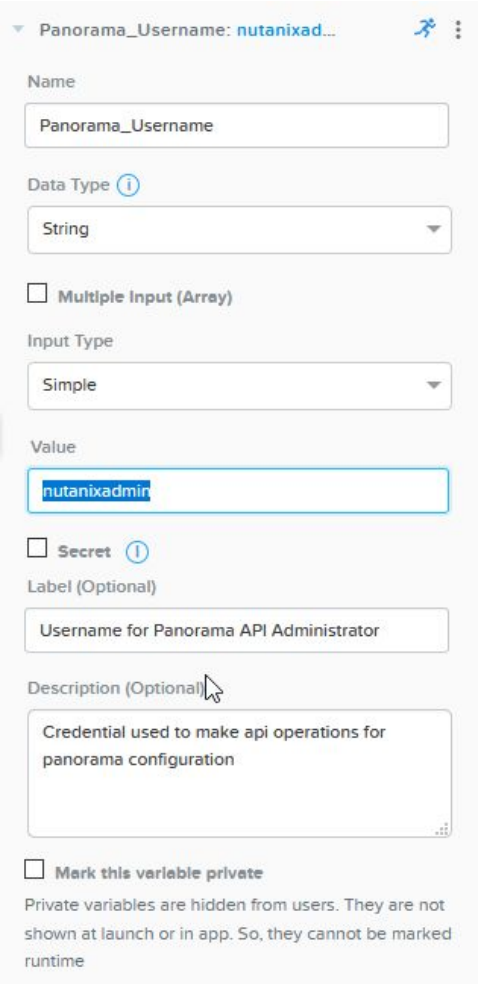
4. Input a numeric value in the *COUNT* section to represent the number of VM-Series instances you want to deploy



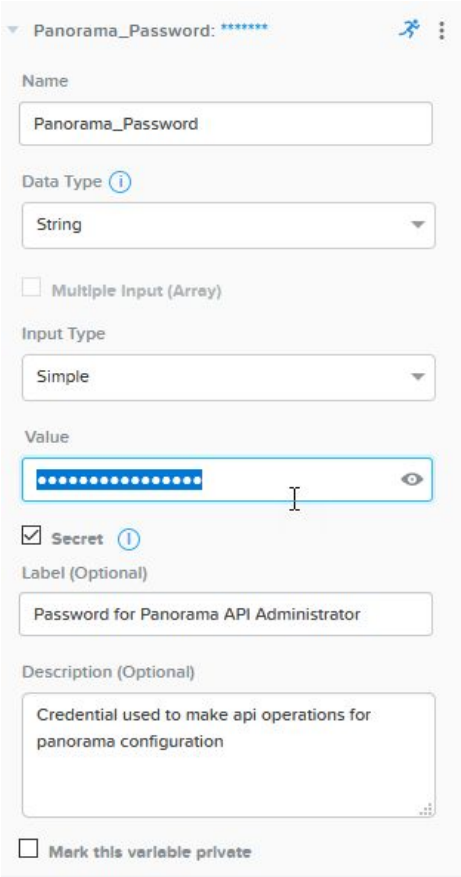
5. Provide the IP address for your Panorama server



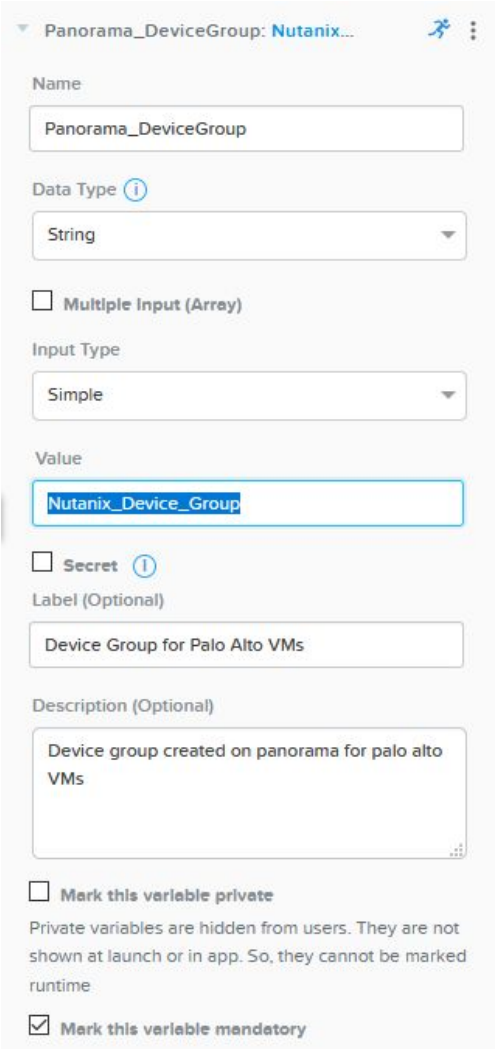
6. Supply the username for the Panorama delegated Administrator account (*nutanixadmin*) created earlier



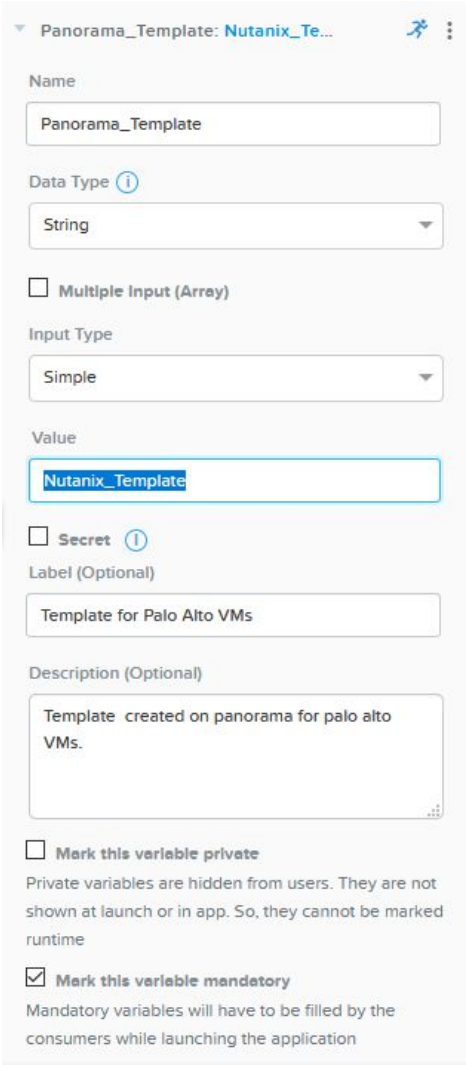
7. Enter the corresponding password for the delegated Administrator account in the *Value* field



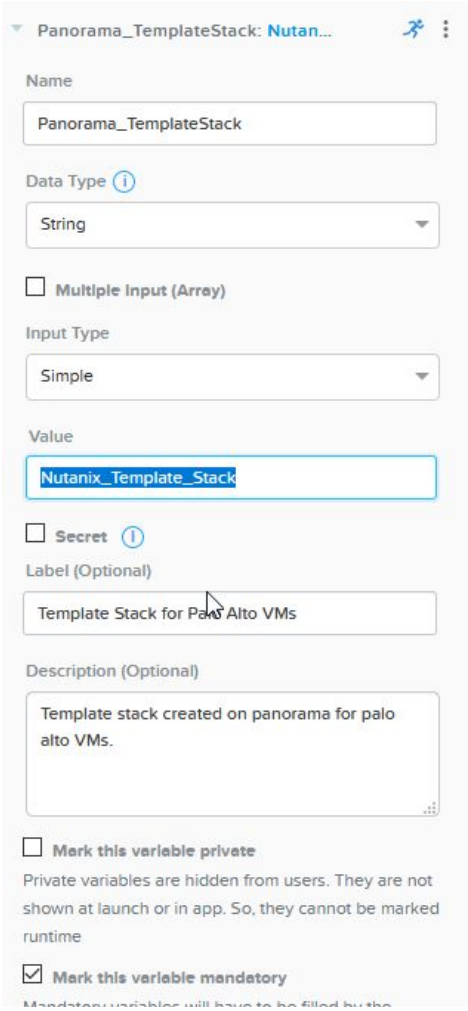
8. Accept the default *Panorama Device Group* name (*CALM*) or supply your own in the *Value* field



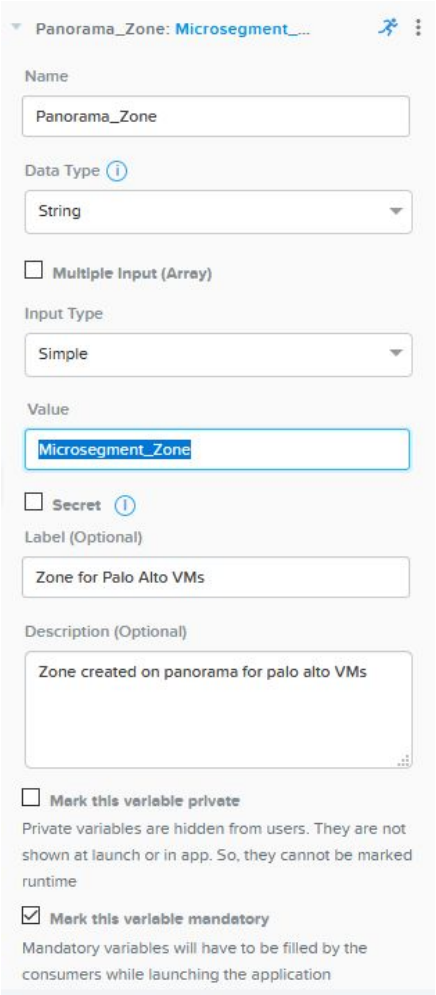
9. Accept the default *Panorama Template* name (*Calm_Template*) or supply your own in the *Value* field



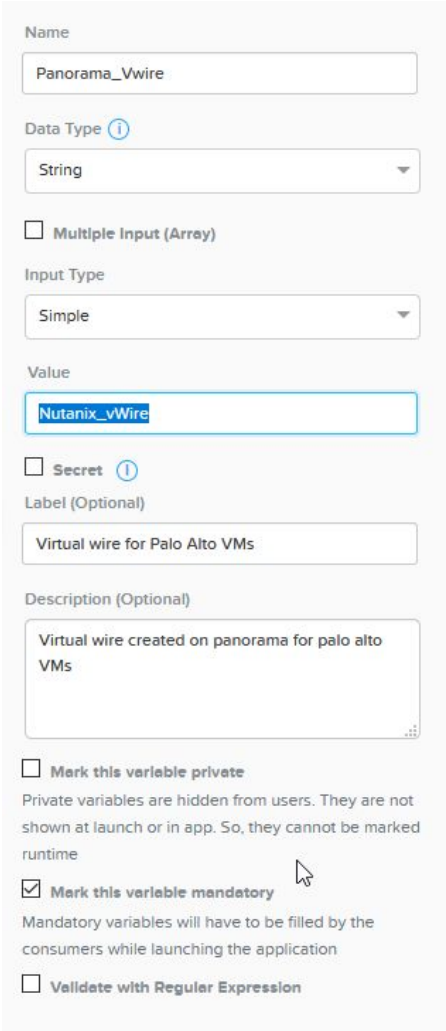
10. Accept the default *Panorama Template Stack* (*Calm_Stack*) or supply your own in the *Value* field



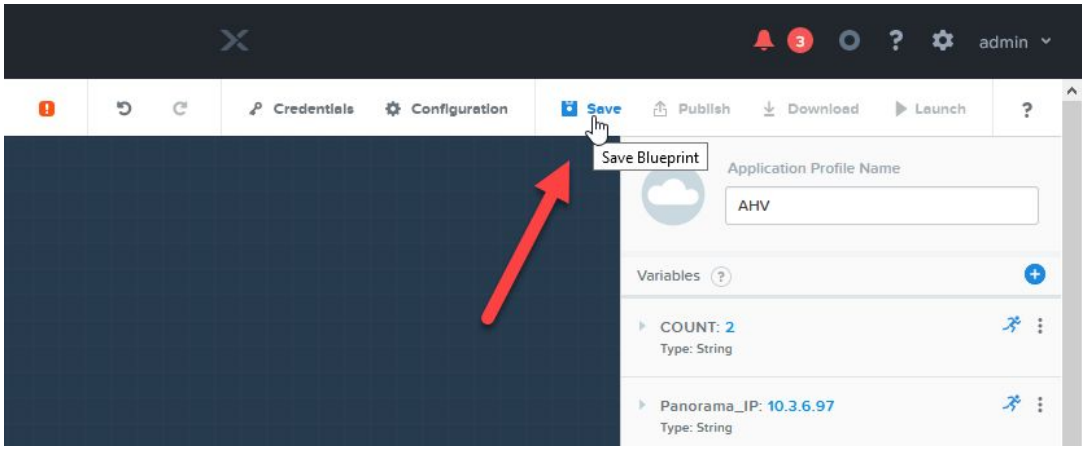
11. In the *Panorama_Zone* section, accept the default *PAN-OS Security Zone Name* (*CALM-VWIRE-ZONE*) or supply your own in the *Value* field



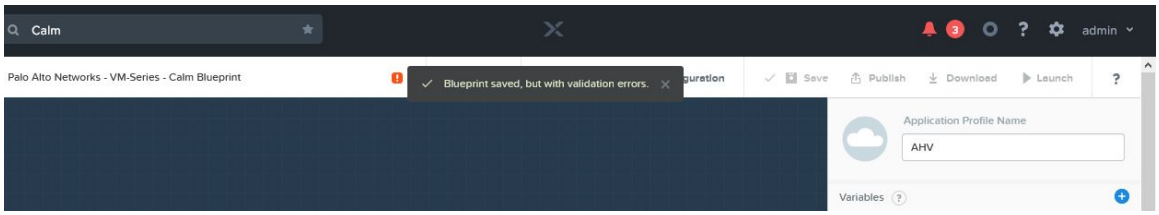
12. In the *Panorama_Vwire* section, accept the default name for the *PAN-OS Virtual Wire* object (*default-vwire*) or supply your own in the *Value* field



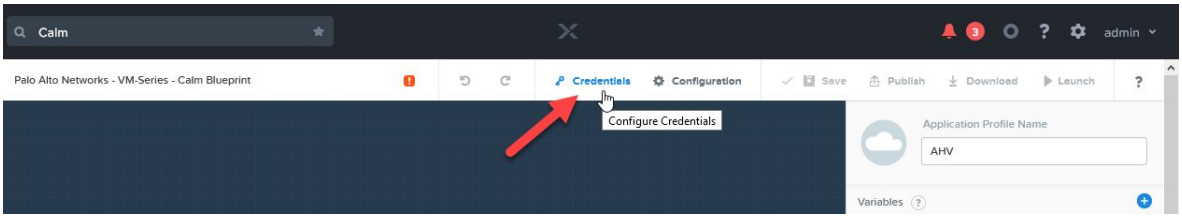
13. Scroll up to the top and click *Save*



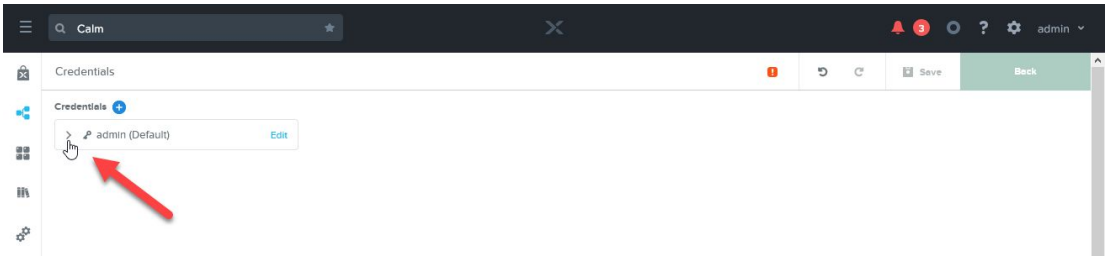
14. You will see an error message displayed – this is expected behavior



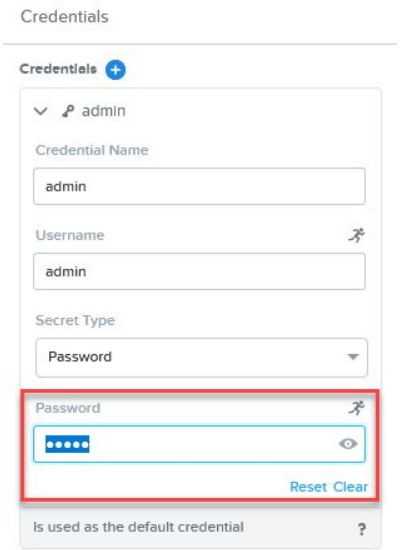
15. Click the *Credentials* link

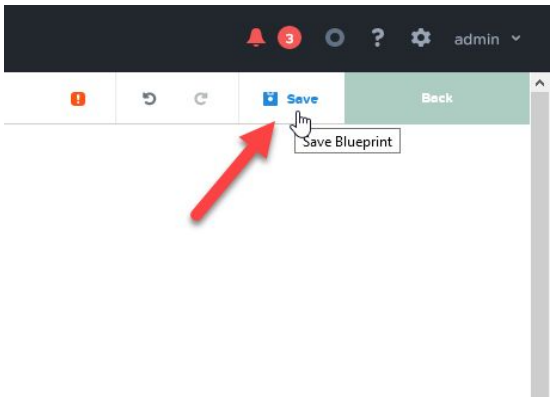


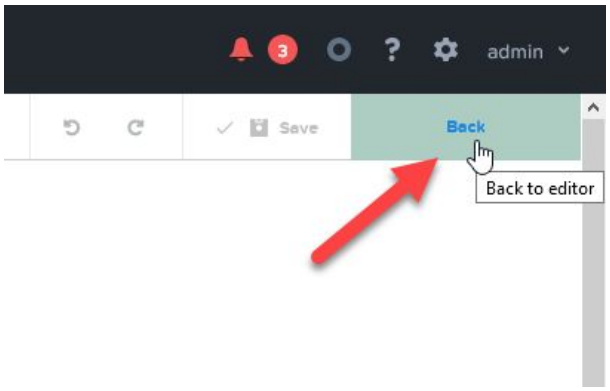
16. Expand the *Credentials* section by clicking the > next to the username *admin*



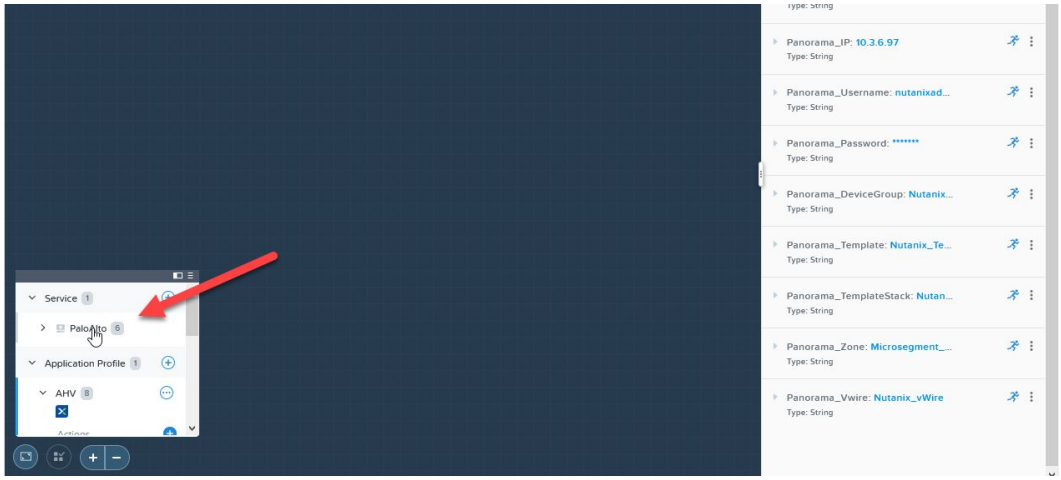
17. Input the default PAN-OS admin password (*admin* – all lowercase) and click *Save* – this time the changes apply without any error message – click the *Back* button



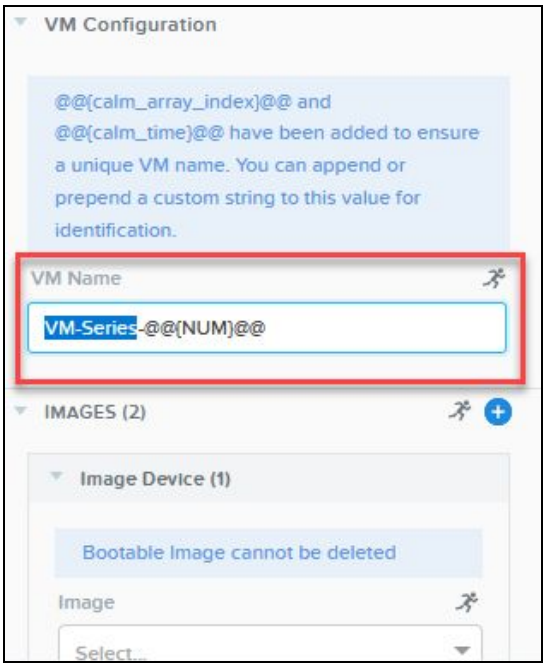




18. In the lower left-hand corner, click the word *PaloAlto* in the box labeled *Service* – a new set of configuration settings will open on the righthand side of the page



19. The names of the *Virtual Machines* are dynamically created based on the value defined in the *VM Configuration* section

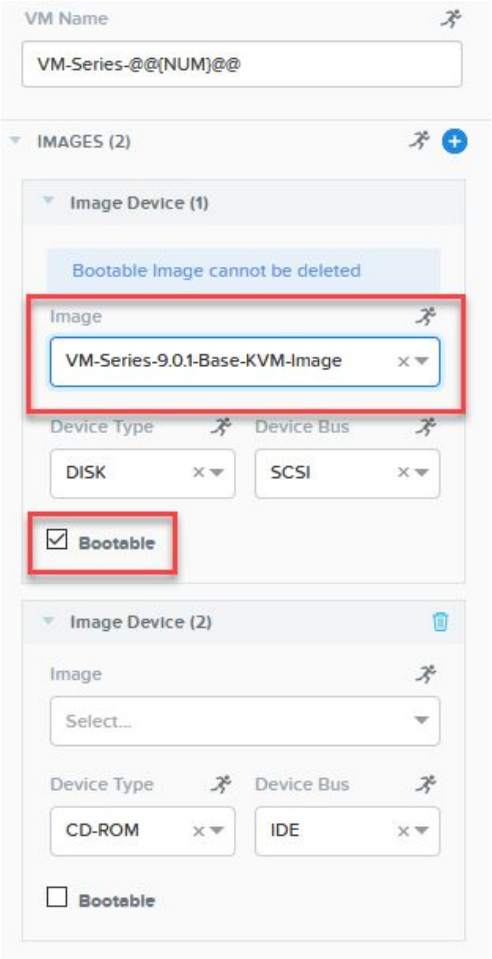


The default text `PaloAlto-@@{NUM}@@` will create *Virtual Machines* in the following format:

```
PaloAlto-1
PaloAlto-2
…
PaloAlto-X
```

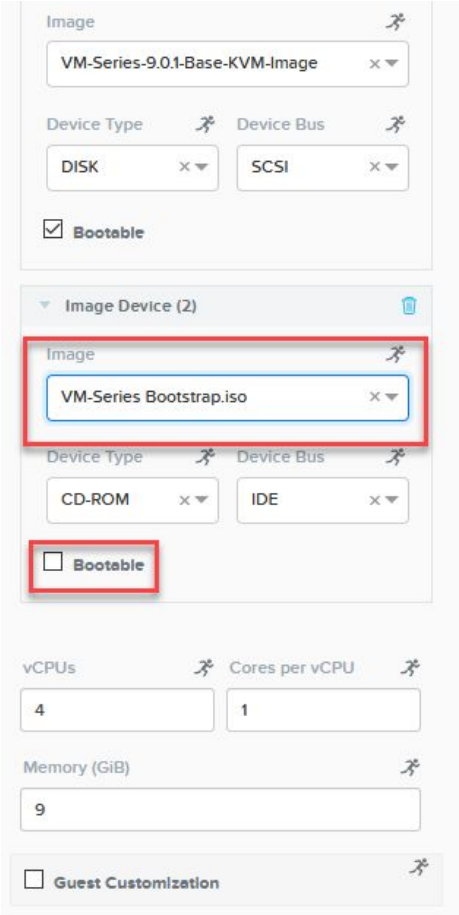
To change the name of the *Virtual Machines*, only replace the text up to `@@{NUM}@@`

20. Modify the drop-down select for *Image Device (1)* to reflect the *PAN-OS for VM-Series KVM Base Image* you imported earlier – **do not uncheck** checkbox next to *Bootable* – the *PAN-OS for VM-Series KVM Base Image* is the default boot volume and the VM will not boot if the checkbox is unchecked



21. Modify the drop-down select for *Image Device (2)* to point to the *Bootstrap ISO* you imported earlier – **do not check** the checkbox next to *Bootable* – the ISO image is only used to provide configuration settings during the provisioning process – the VM never boots from the ISO image

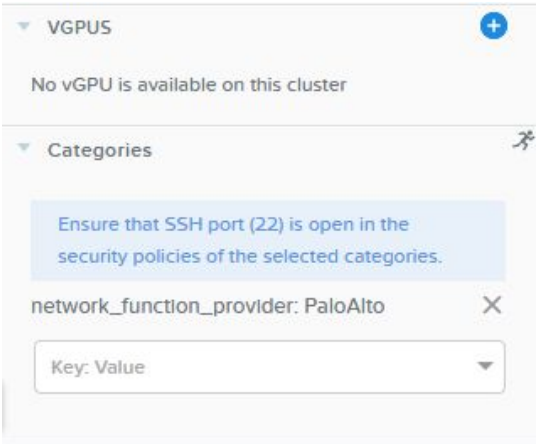
The default values for *VCPUs* (4), *Cores* (1), and *Memory* (9 GB) are valid for a Palo Alto Networks VM-Series VM-100, VM-200, or VM-300 license.



***NOTE**: If you intend to deploy another VM-Series license, please review the Palo Alto Networks VM-Series System Requirements documentation for the required resources:*

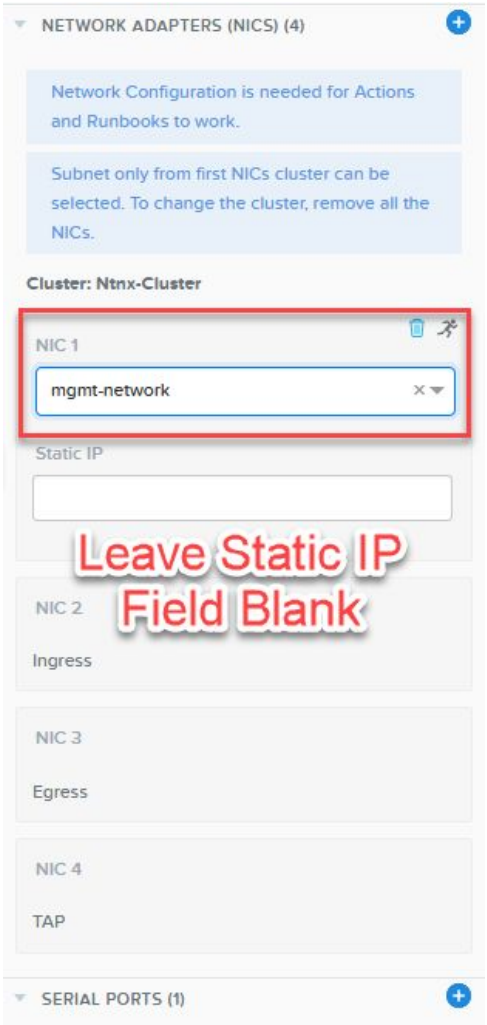
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-models/vm-series-system-requirements.html

22. Leave the value for *network_function_provider: PaloAlto* blank



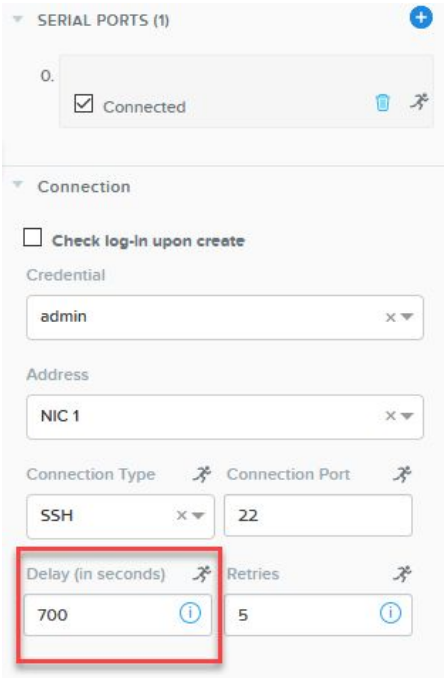
23. In the *Network Adapters* section, choose the *Network* as defined in the *Project* created earlier for *NIC1* (VM-Series management interface)

***NOTE**: Do not configure a Static IP address – the Nutanix Calm automation framework operates optimally when IP addresses are assigned via DHCP*



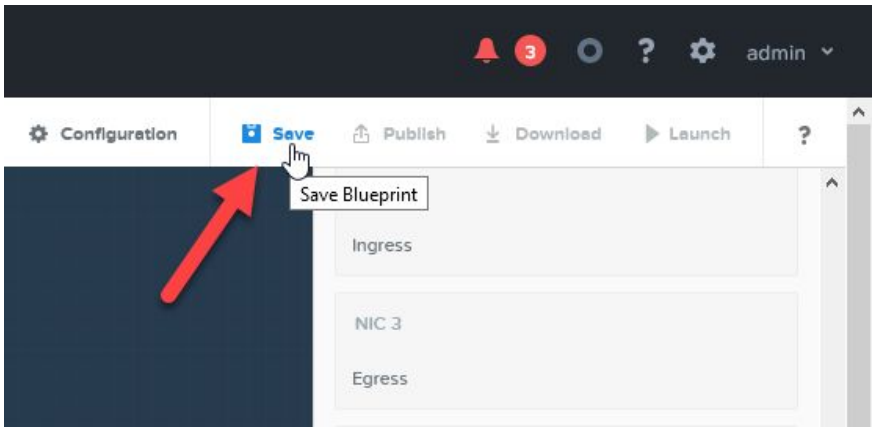
24. Do not uncheck the checkbox in the *Serial Ports* section – this will cause significant delays in the amount of time it takes for the VM-Series instances to boot

25. It is not necessary to configure any additional settings as the default values are optimized for deployment in the majority of Nutanix customer's environments ***



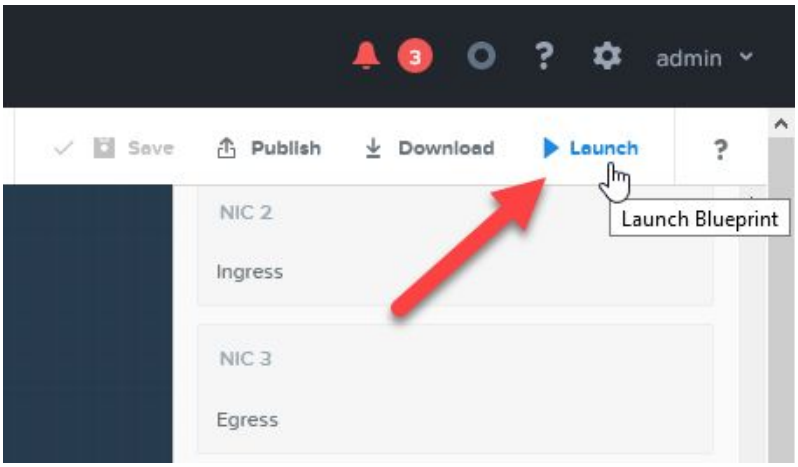
**** in some rare cases where the Nutanix AHV cluster nodes operate at high utilization rates, it may be necessary to increase the default timeout value from 700 (seconds) to 800 or 900. Increasing the timeout value does not negatively affect the deployment of VM-Series in any way. It provides additional time for PAN-OS XML API programmatic functions to finish processing.*

26. Scroll to back to the top and click Save

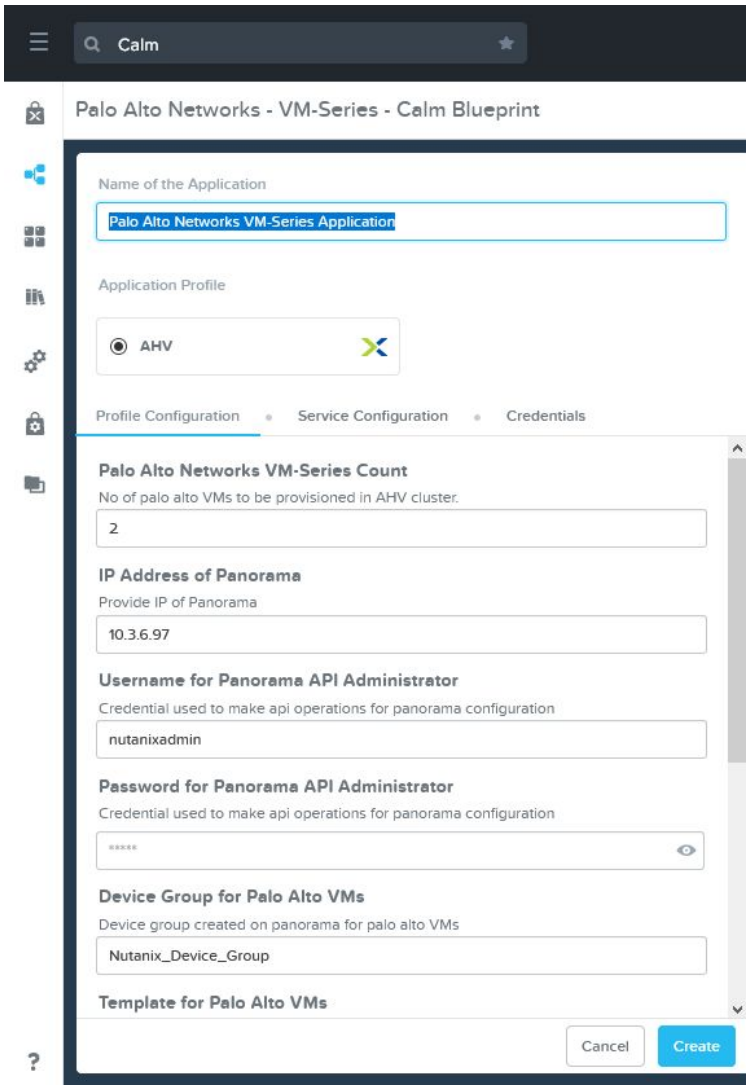


Deploy Palo Alto Networks VM-Series Application from Calm Blueprint

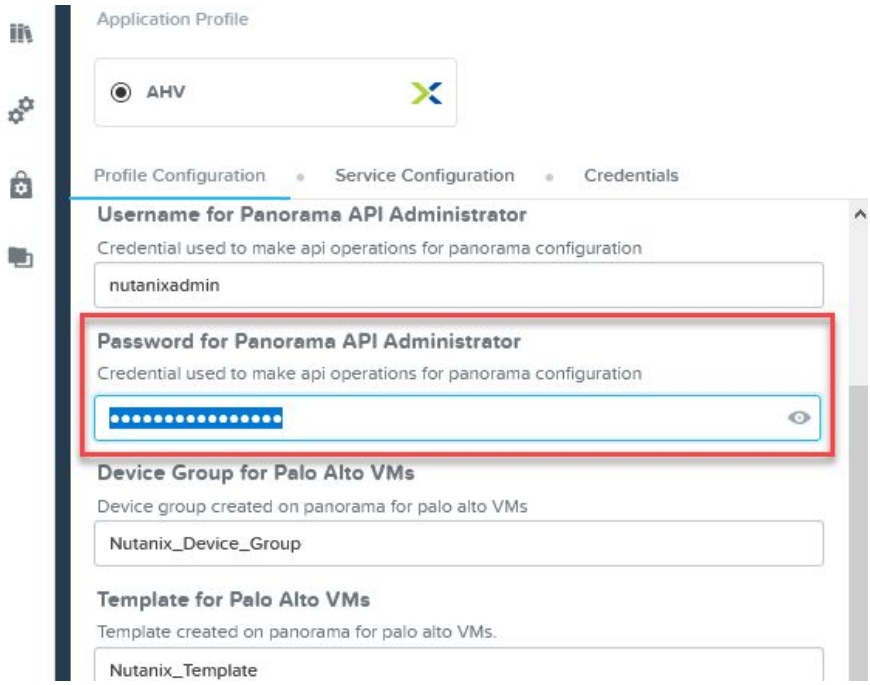
1. Once the settings for the Nutanix Calm Blueprint for Palo Alto Networks VM-Series save completely, click the *Launch* button



2. On the next screen, review the settings to ensure accuracy

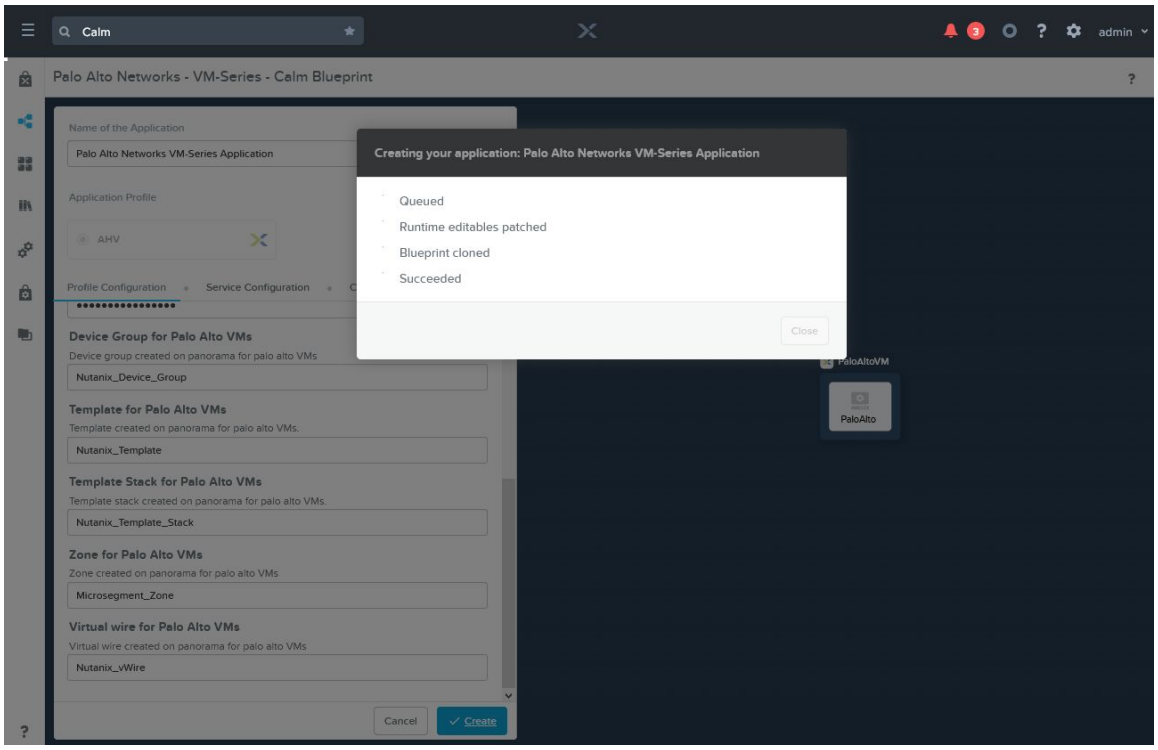


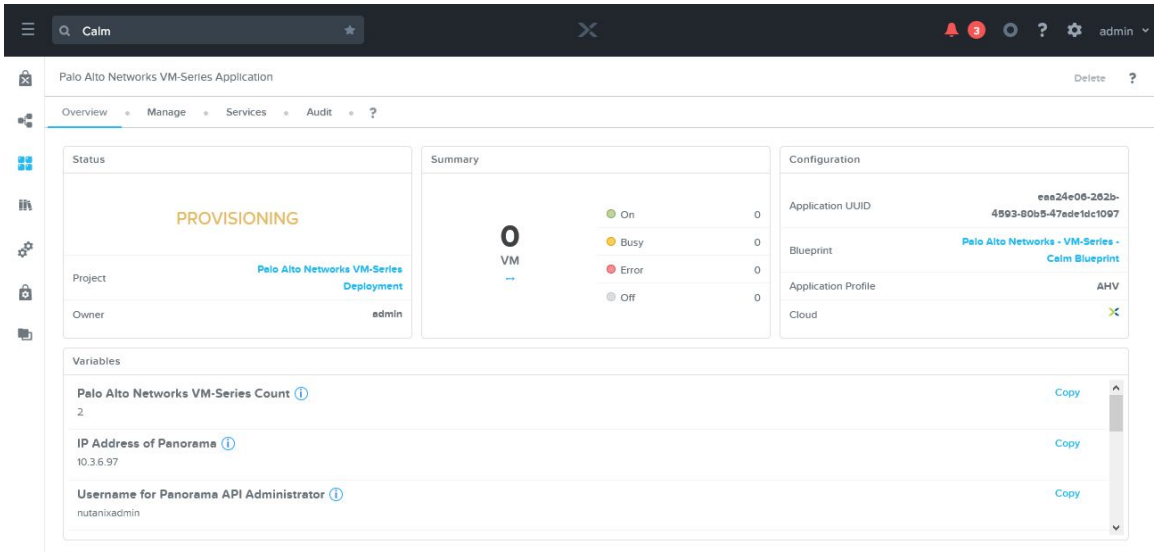
3. Confirm the password for the delegated Administrator account

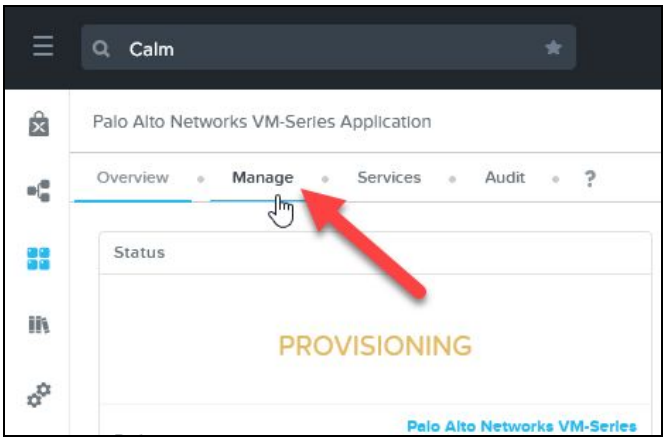


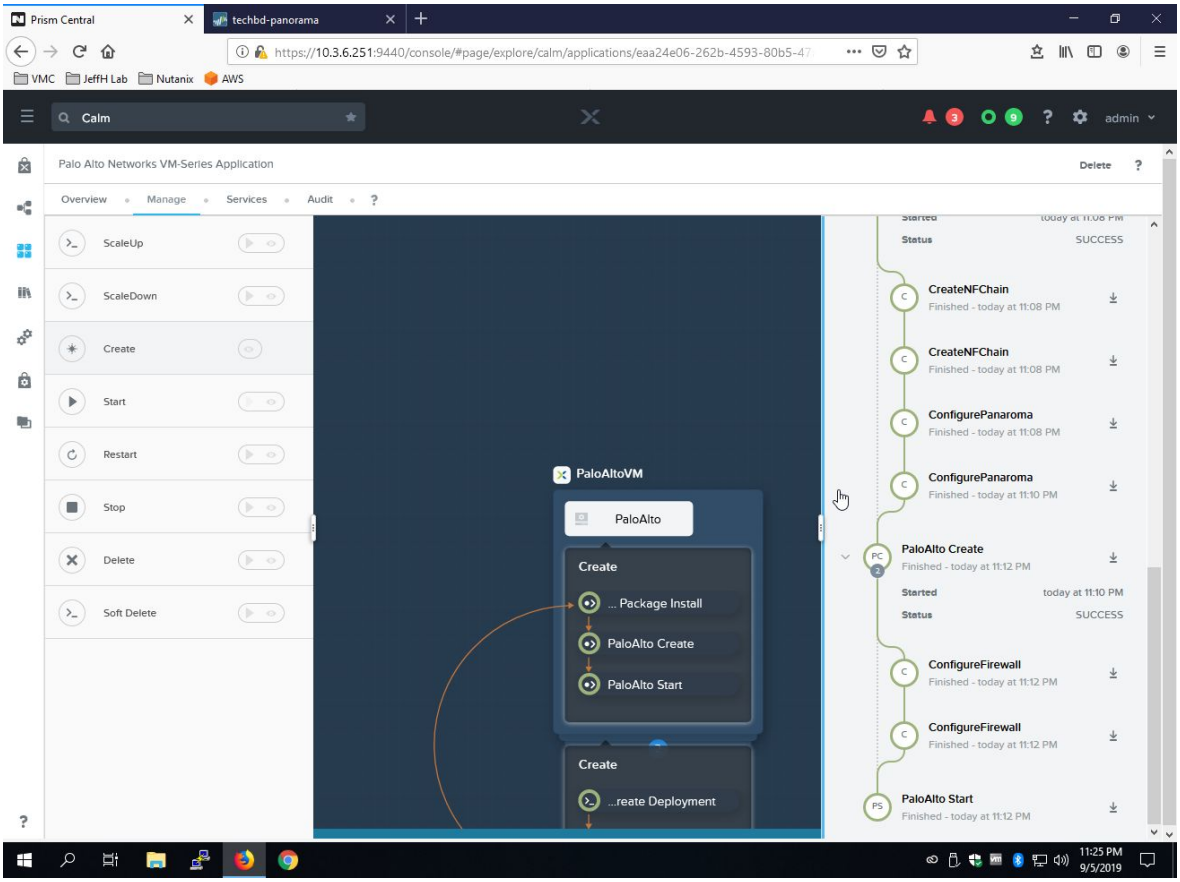
4. Click the *Create* button to deploy VM-Series

5. You can switch to the *Manage* tab to follow along with the process


Calm
admin
Palo Alto Networks - VM-Series - Calm Blueprint
Name of the Application
Palo Alto Networks VM-Series Application
Application Profile
AHV
Profile Configuration
Service Configuration
Device Group for Palo Alto VMs
Device group created on panorama for palo alto VMs
Nutanix_Device_Group
Template for Palo Alto VMs
Template created on panorama for palo alto VMs.
Nutanix_Template
Template Stack for Palo Alto VMs
Template stack created on panorama for palo alto VMs.
Nutanix_Template_Stack
Zone for Palo Alto VMs
Zone created on panorama for palo alto VMs
Microsegment_Zone
Virtual wire for Palo Alto VMs
Virtual wire created on panorama for palo alto VMs
Nutanix_vWire
Cancel
Create
Creating your application: Palo Alto Networks VM-Series Application
Queued
Runtime editables patched
Blueprint cloned
Succeeded
Close
PaloAltoVM
PaloAlto


Calm
admin
Palo Alto Networks VM-Series Application
Delete
Overview
Manage
Services
Audit
Status
PROVISIONING
Project
Palo Alto Networks VM-Series Deployment
Owner
admin
Summary
0
VM
On 0
Busy 0
Error 0
Off 0
Configuration
Application UUID
eaa24e06-262b-4593-80b5-47ade1dc1097
Blueprint
Palo Alto Networks - VM-Series - Calm Blueprint
Application Profile
AHV
Cloud
Variables
Palo Alto Networks VM-Series Count
2
Copy
IP Address of Panorama
10.3.6.97
Copy
Username for Panorama API Administrator
nutanixadmin
Copy

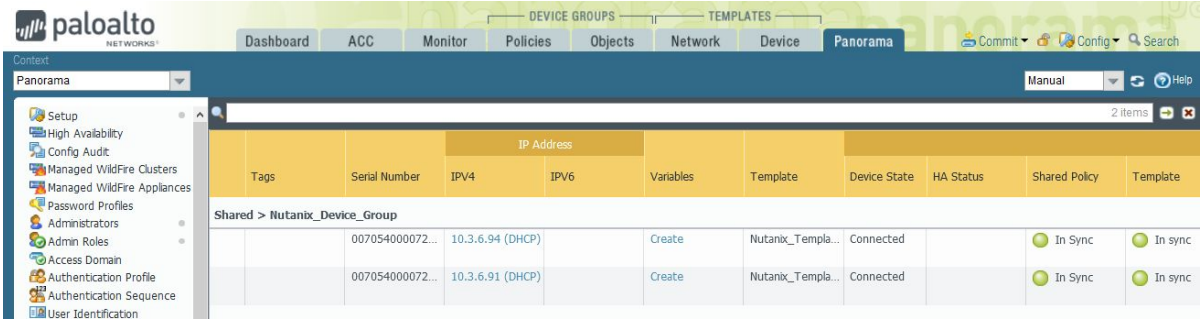




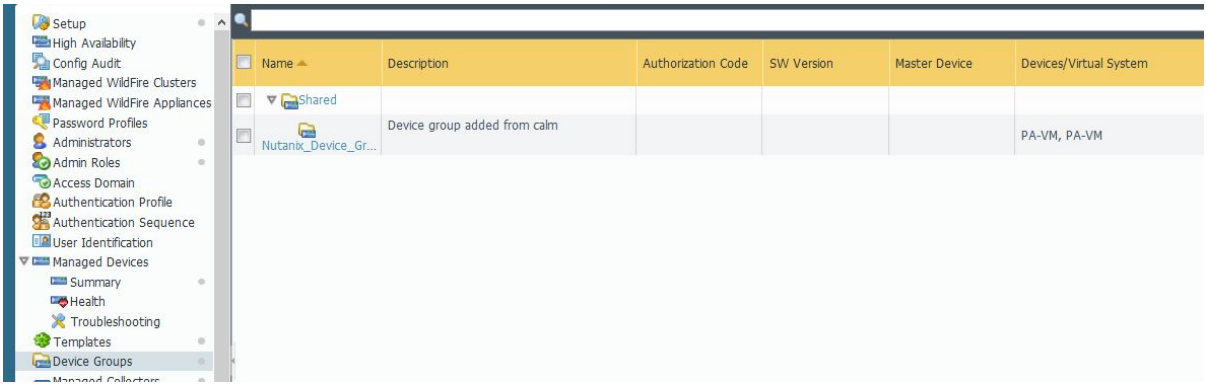
Verify PAN-OS XML API Configuration Settings

Switch to the Panorama Web UI to verify Nutanix Calm provisioned the following settings:

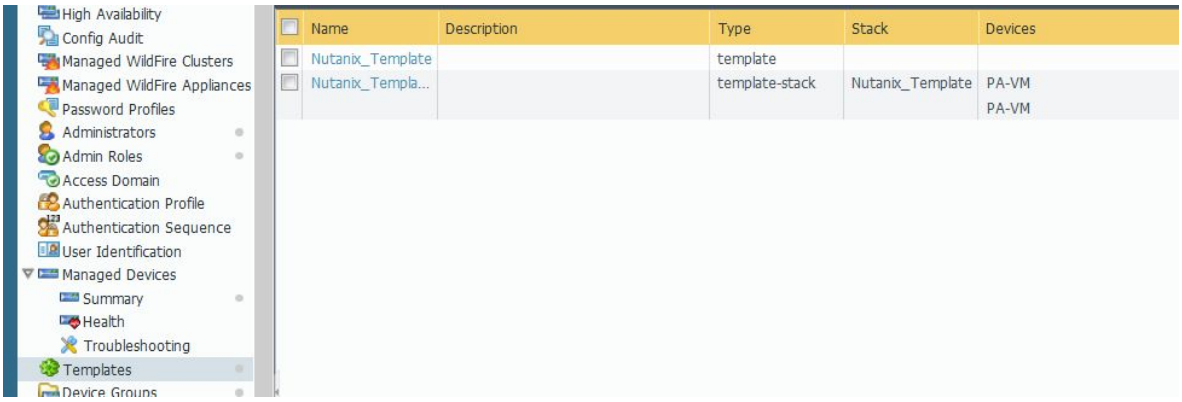
- VM-Series are Registered (Managed Devices -> Summary)



- Device Group is provisioned



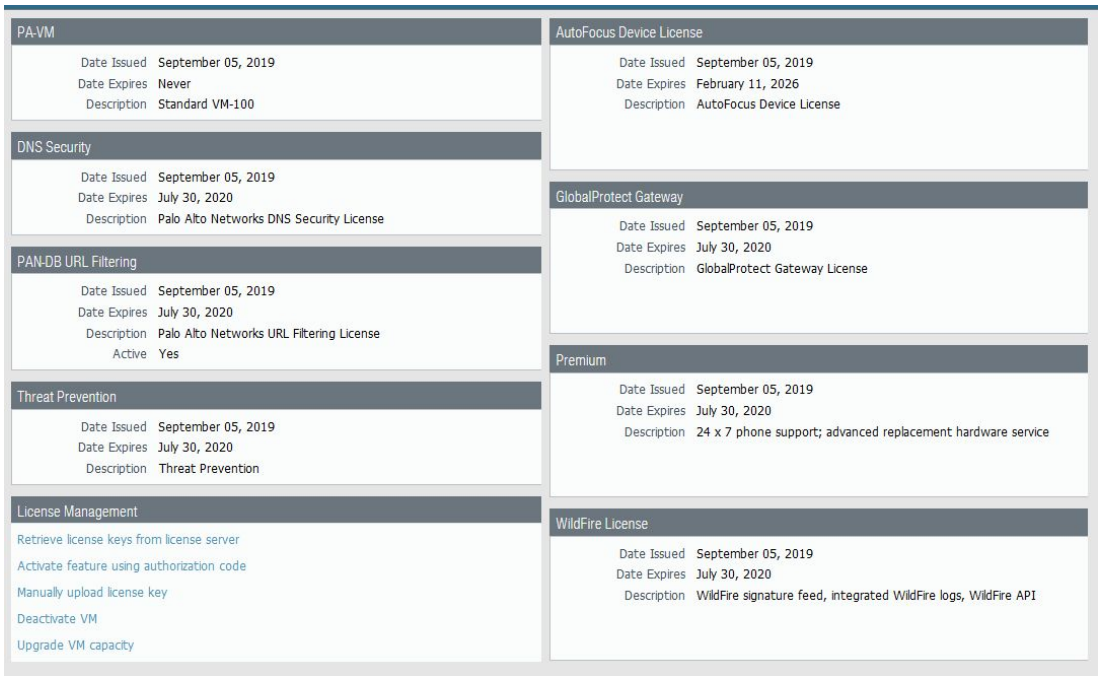
- Template and Template Stack are provisioned



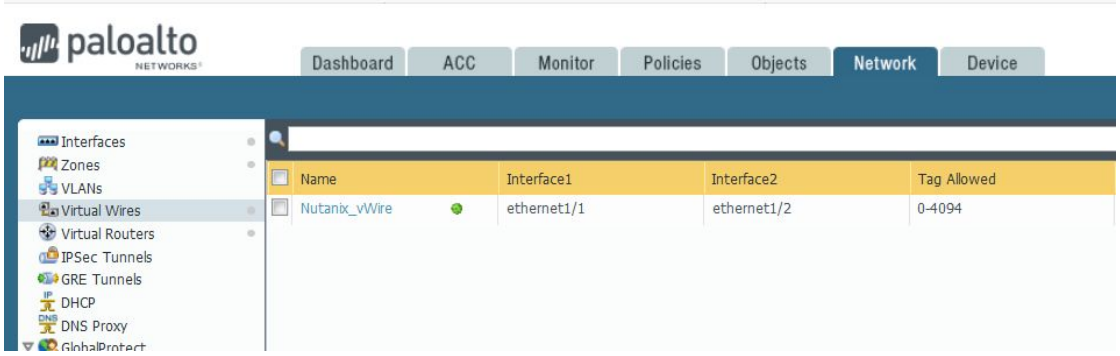
Verify VM-Series Virtual Machines Provisioning

Switch to the VM-Series Web UI for each instance deployed to verify the following:

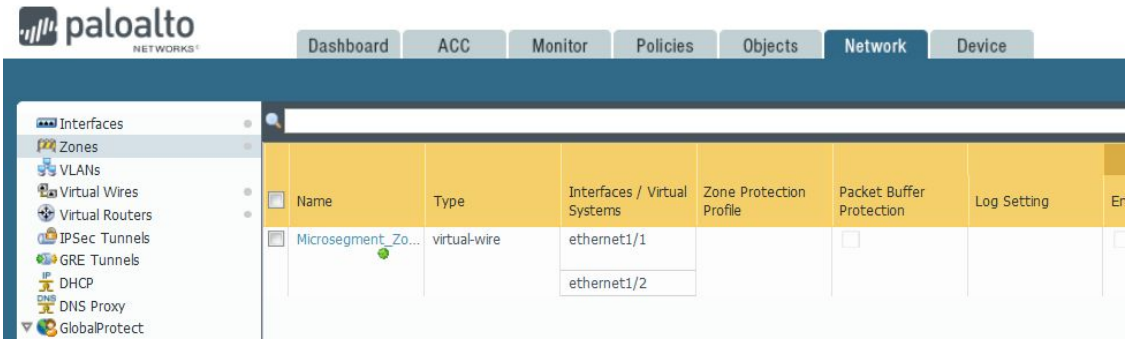
- Licenses activated



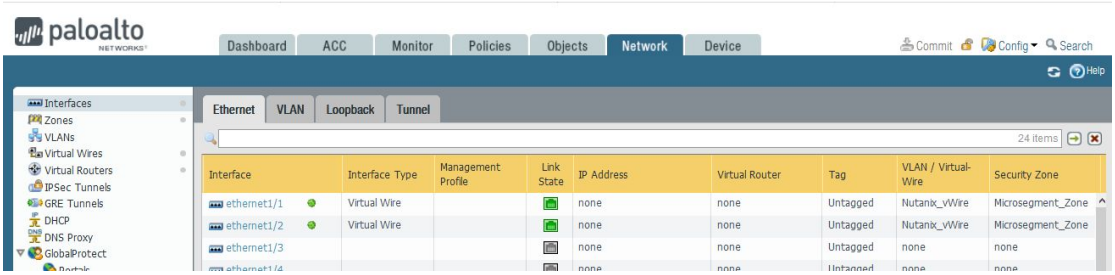
- Virtual Wire



- Security Zone



- Network Interfaces



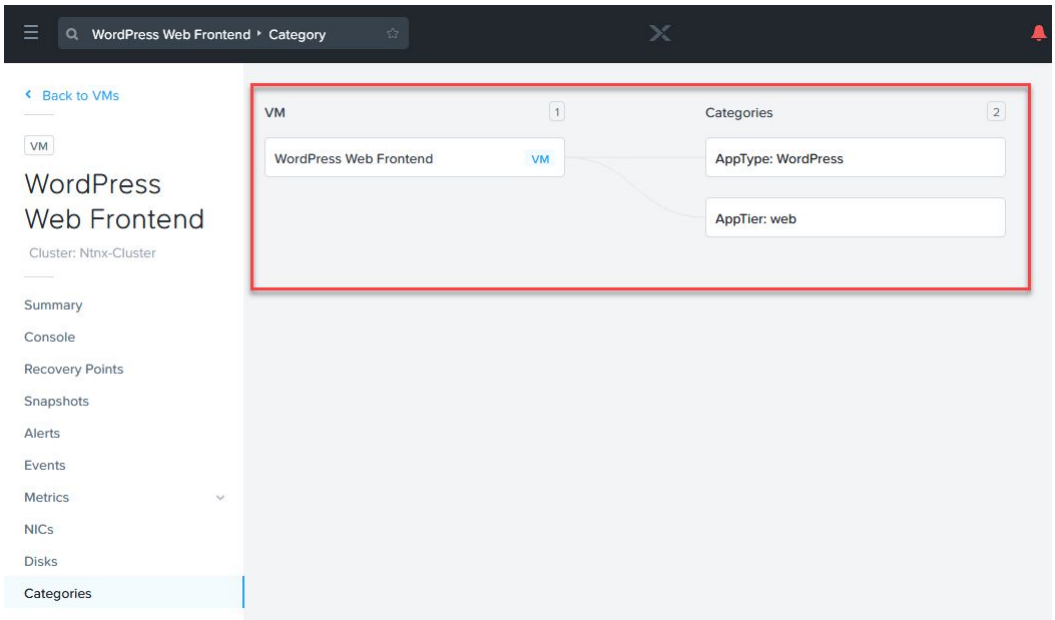
Apply Microsegmentation Policy via Nutanix Flow and VM-Series

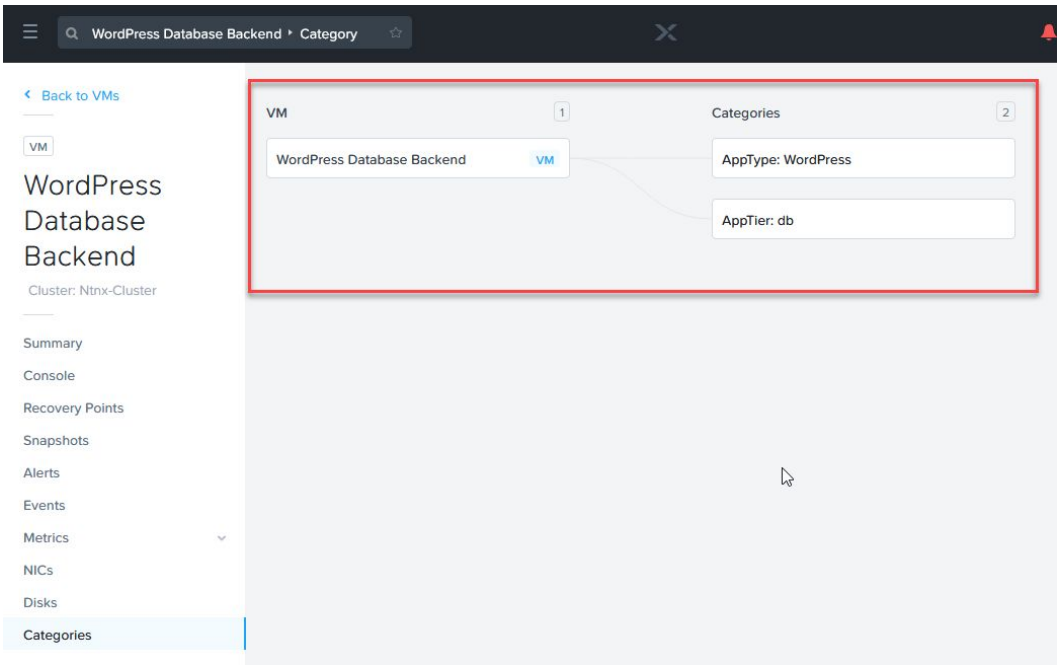
Nutanix provides a framework whereby traffic between virtual machines can be redirected through Nutanix Flow for traditional traffic enforcement via an integrated firewall that processes traffic at layer-4 based on source/destination port and protocol.

For customers that want to reap the benefits of Palo Alto Networks Next-Generation Firewall, deploying VM-Series on Nutanix AHV with the Calm Blueprint automatically creates a Service Chain. The Service Chain allows customers to transparently redirect traffic at the Virtual NIC driver layer to VM-Series for low latency packet redirection to Palo Alto Networks' industry-leading application layer firewall.

Applying Application and Category objects to your applications allows the administrator to quickly and easily control traffic flows between workloads. In the following example, we secure a two-tier deployment of WordPress. The tiers are separated into a web tier and a database tier. The WordPress front-end web and application server are deployed on one Virtual Machine while the MySQL database is deployed on another Virtual Machine.

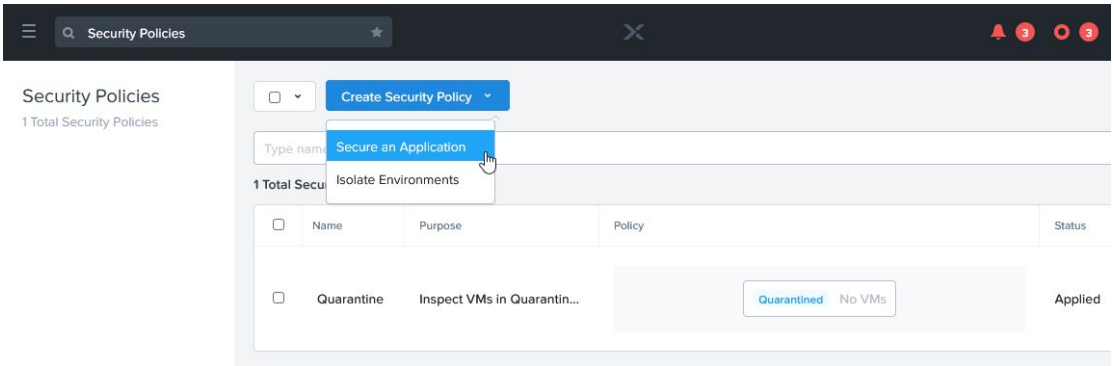
An Application object is defined to represent WordPress as an application (*AppType: WordPress*) and is further divided into two categories – the web tier (*AppTier: web*) and the database tier (*AppTier: db*). The Application object and Category objects are applied to the two Virtual Machines.



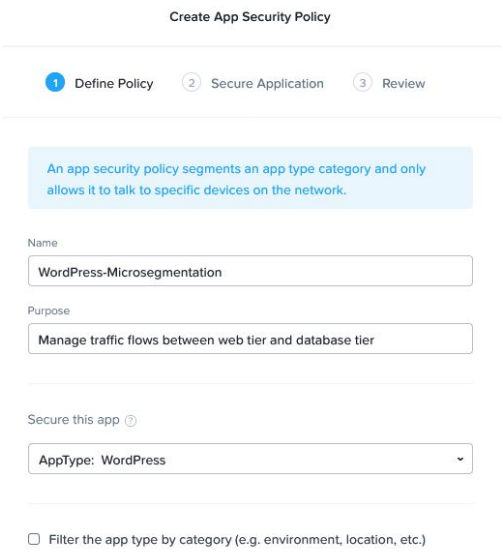


We create a Security Policy in Nutanix Flow to quickly and easily apply a Microsegmentation policy to control the east/west traffic flows between the WordPress web application server and the WordPress database server.

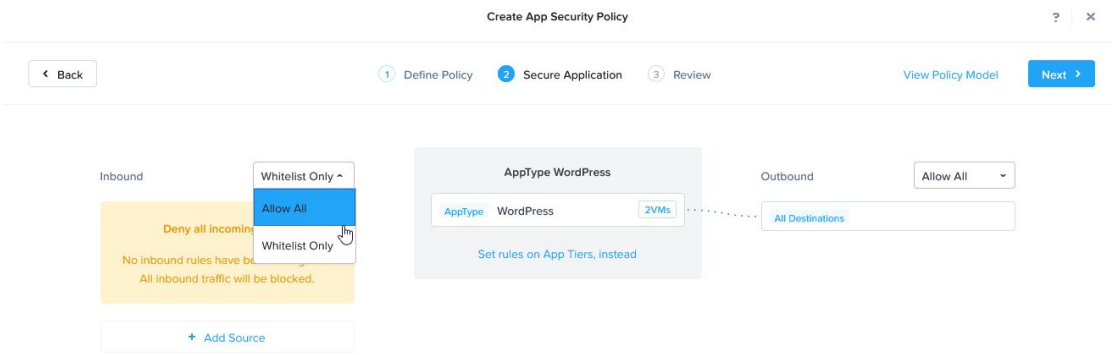
1. Navigate to *Policies -> Security Policies*
2. Click *Create a Security Policy* and choose *Secure an Application*



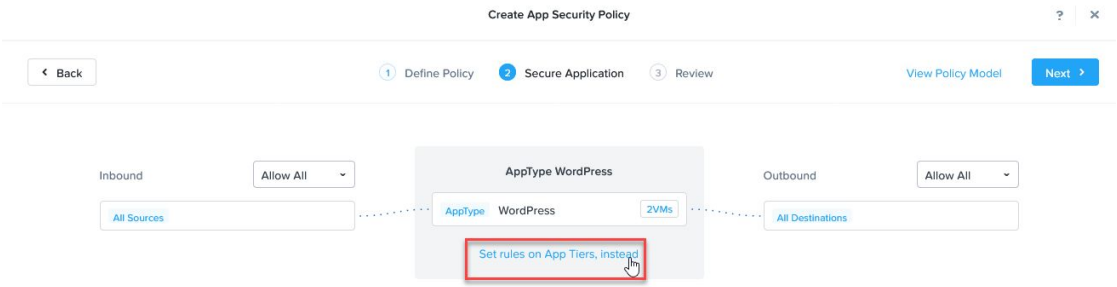
3. Provide a *Name* and *Description* for the new security policy, then choose *App Type: WordPress* in the drop-down select, then click *Next*



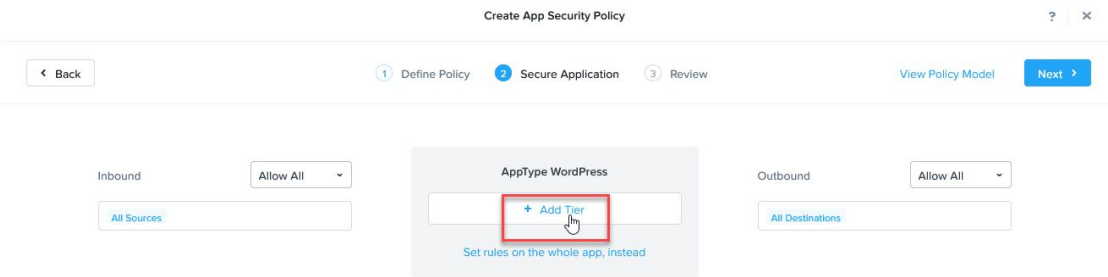
4. Since we already have a Palo Alto Networks Next-Generation Firewall securing the north/south traffic at the perimeter, select the *Whitelist Only* drop-down select and choose *Allow All*



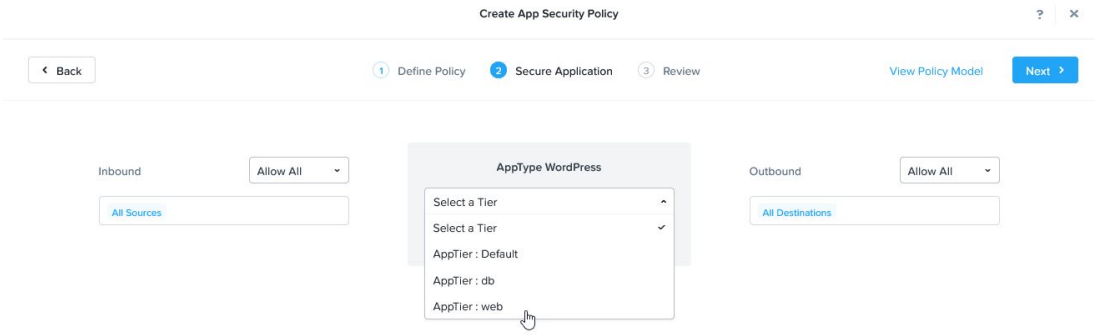
5. In the center column, select *Set Rules on App Tiers* instead



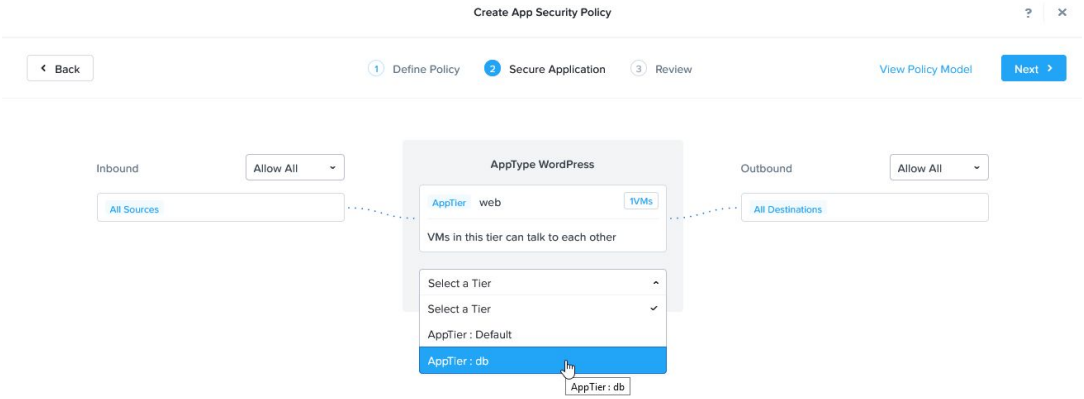
6. Click *+ Add Tier*



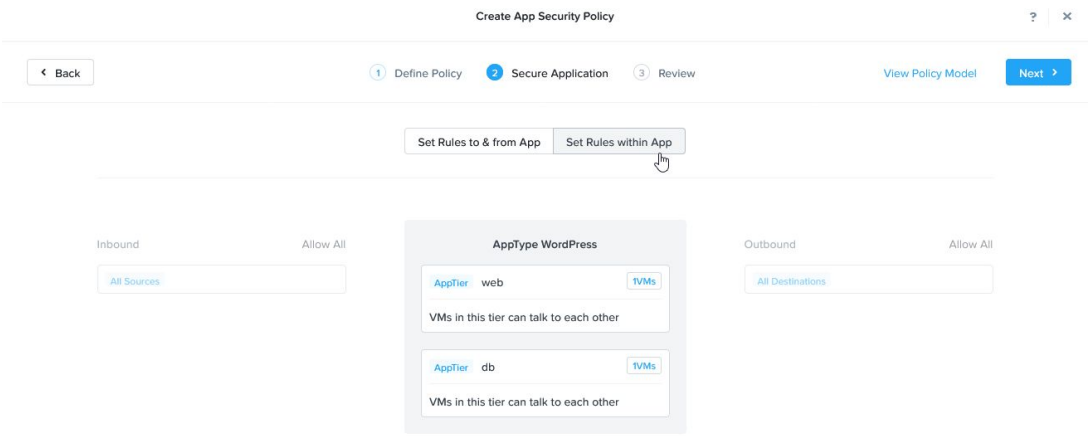
7. Select *App Tier: web*



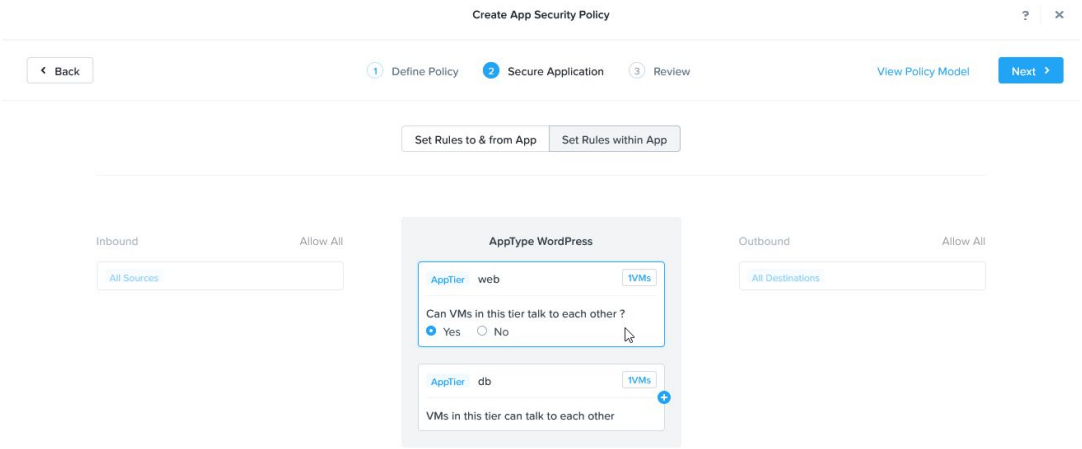
8. Click *+ Add Tier* and select *App Tier: db*



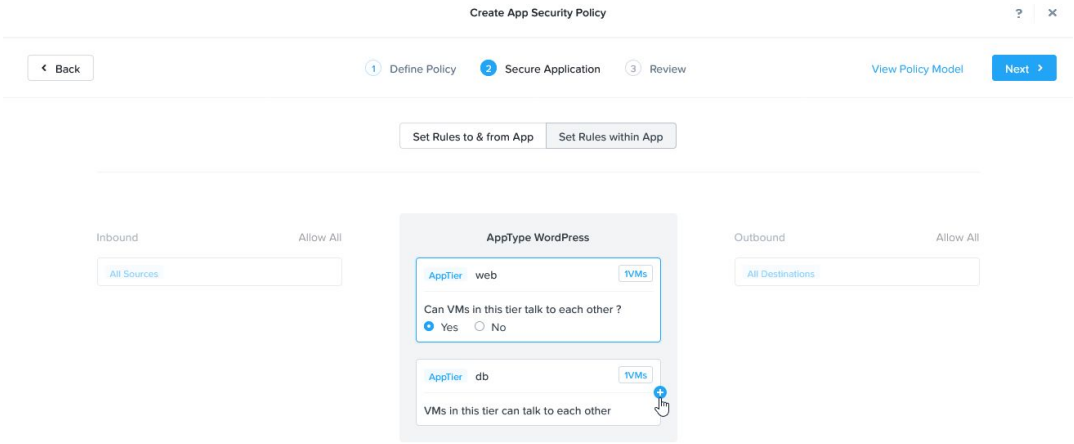
9. Select *Set Rules within App*



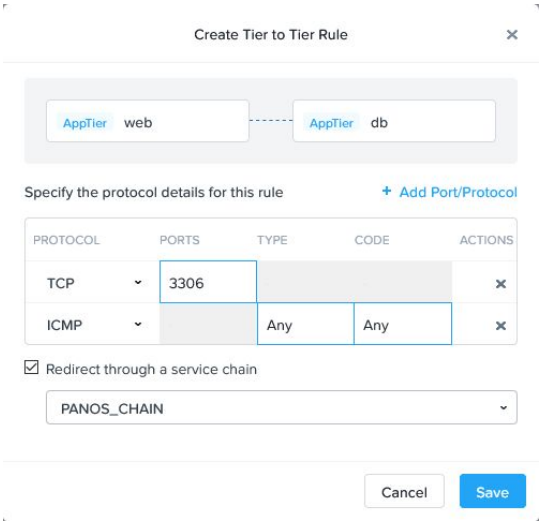
10. Click on the rectangle representing *AppTier: web* to select it – a blue outline will appear



11. Click the *+* sign on the right side of *AppTier: db*



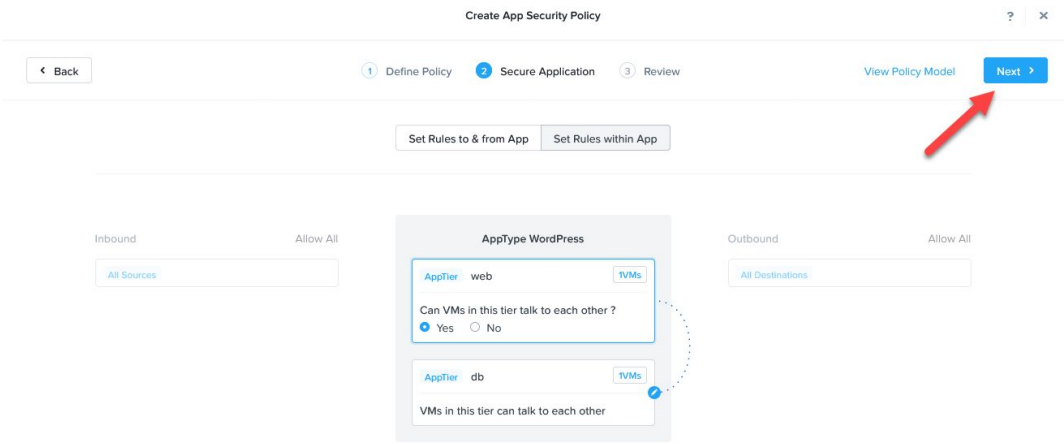
12. In the Create Tier to Tier Rule that appears, enter the TCP/UDP/ICMP traffic flows to redirect to VM-Series via the *Service Chain*, check the box next to *Redirect through a service chain*, and then select *PANOS_CHAIN* in the drop-down select



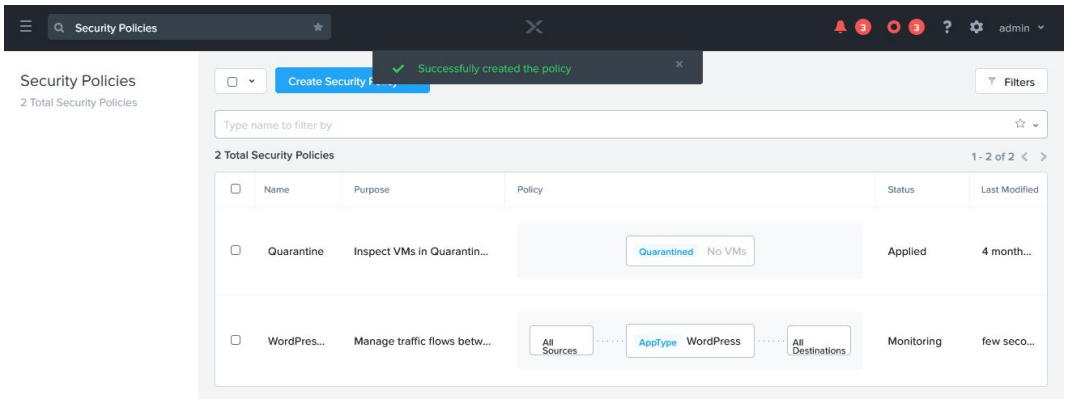
In this rule, both MySQL (*3306/tcp*) and all *ICMP* traffic is redirected to VM-Series

13. Click *Save* to add the rule

14. Click *Next*



15. Choose either *Save and Monitor*, or if you are ready to enforce the new *Tier to Tier* rule with VM-Series, simply click *Apply Now*



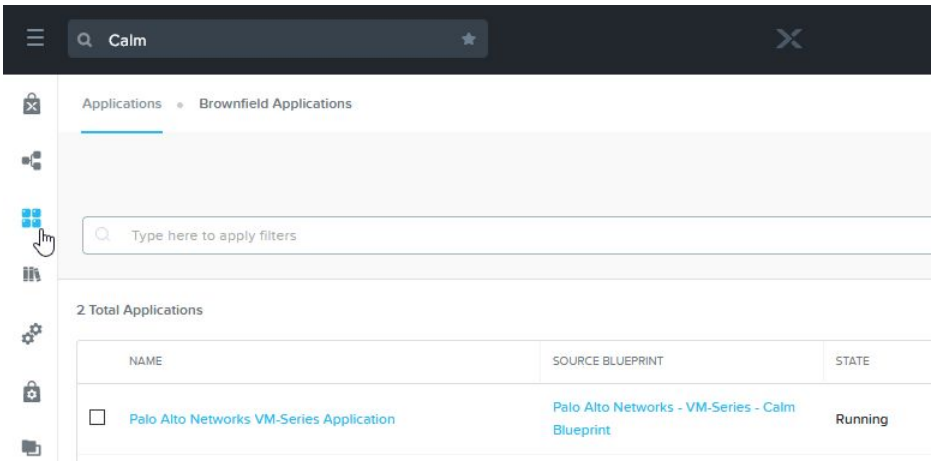
16. Switch to the VM-Series firewall *Monitor* tab for the appropriate firewall – or if you have centralized logging configured in Panorama, view the *Traffic* logs on the *Monitor* tab within the Panorama admin interface

Deploy Additional VM-Series via Calm Scale Out

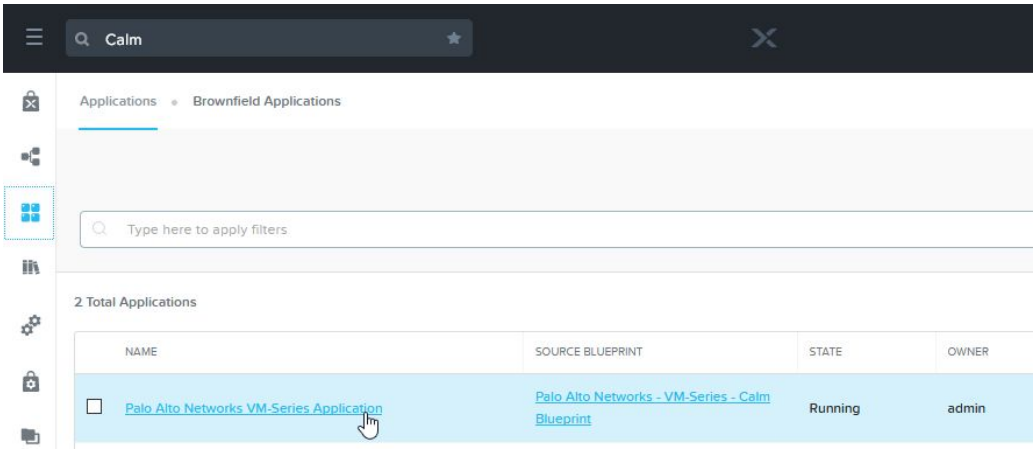
As your workloads scale up, so does the number of Nutanix AHV cluster nodes in your environment. The Nutanix scale-out capability provides a method for administrators to add additional VM-Series instances to an existing deployment with only a few clicks.

The following example builds upon the two VM-Series instances we deployed to a Nutanix AHV cluster. To increase the scalability of the environment, we will leverage the Nutanix Calm Scale Up action to add an additional two instances of VM-Series across the AHV cluster.

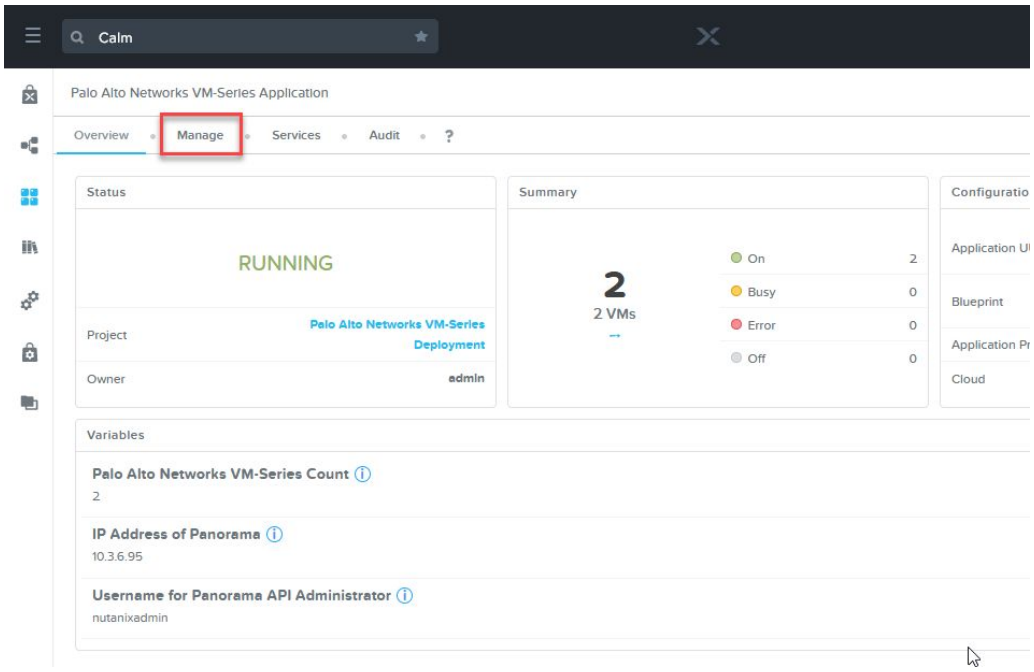
1. Navigate to *Calm -> Applications*



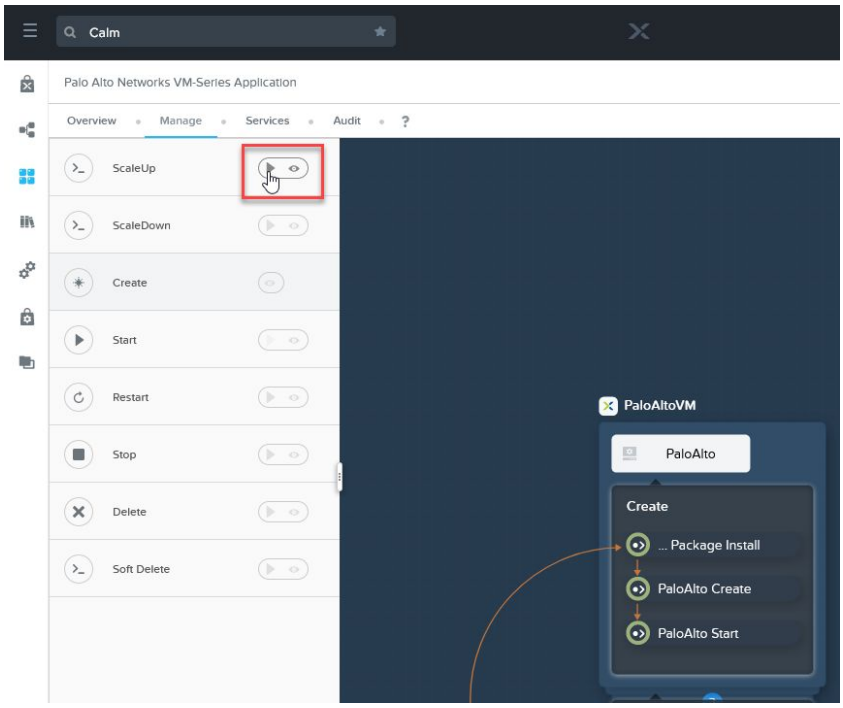
2. Open the *Palo Alto Networks VM-Series Application*



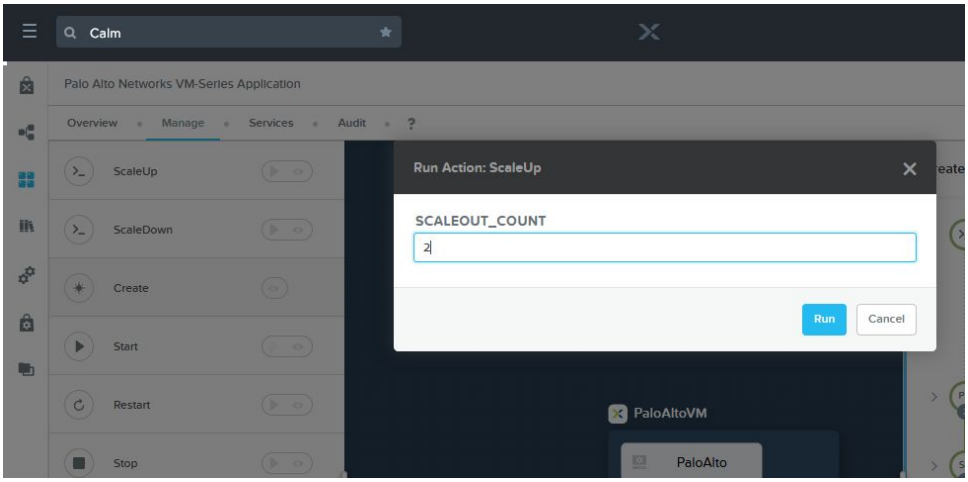
3. Select the *Manage* tab



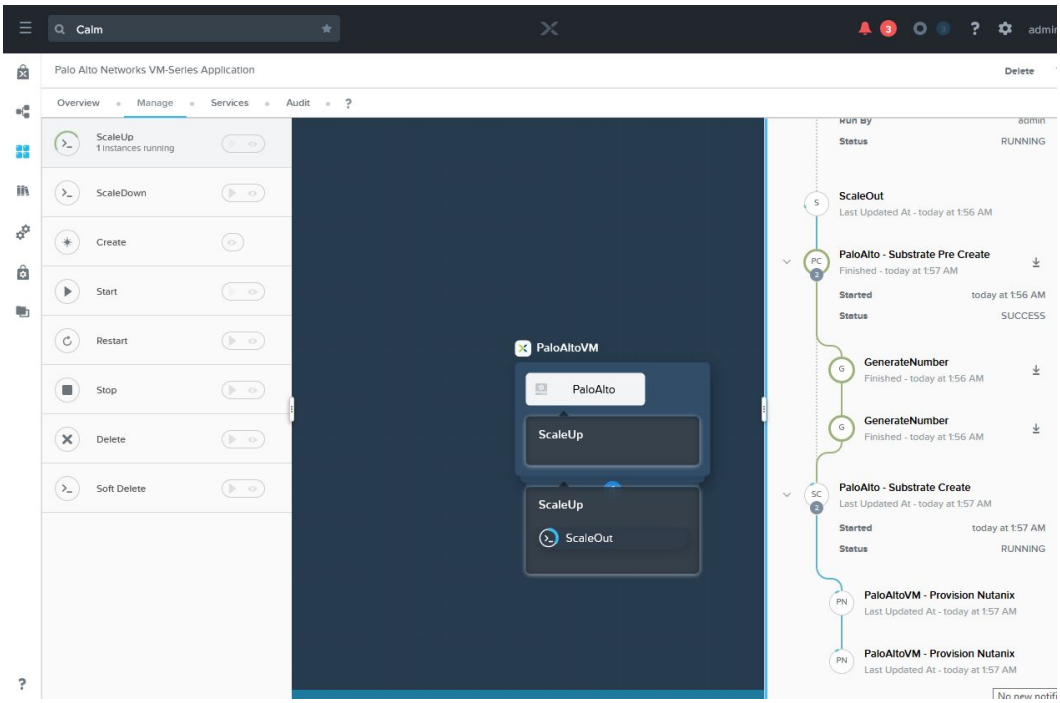
4. Click the > in the *ScaleUp* pane



5. Modify the *SCALEOUT_COUNT* to reflect the total number of additional VM-Series instances to deploy



6. Click *Run*



That's it! Nutanix Calm will automatically:

- Provision the desired number of additional VM-Series instances
- Automate licensing of the additional VM-Series appliances
- Subscribe the newly created instances to the same Panorama server
- Add the new instances to the same Panorama Device Group, Template, and Template Stack as the existing instances
- Automatically commit the configuration
- Modify the *Service Chain* to allow traffic to be seamlessly redirected to the newly deployed VM-Series instances

Troubleshooting Resources & Documentation

Nutanix

- Nutanix Flow - Tech Note
- Nutanix Calm Reference Architecture
- Nutanix Support Portal
- Blueprints Management - Nutanix Support Portal
- Blueprints Usage - Nutanix Support Portal
- Nutanix: Network Microsegmentation Demo - YouTube
- Tech TopX: Datacenter Security with Flow

Palo Alto Networks

- Palo Alto Networks Support Site
- Create a Support Account - VM-Series Deployment Guide
- License the VM-Series Firewall - VM-Series Deployment Guide
- Activate the License - VM-Series Deployment Guide
- Bootstrap the VM-Series Firewall - VM-Series Deployment Guide
- Generate the VM Auth Key on Panorama - VM-Series Deployment Guide
- Prepare the Licenses for Bootstrapping - VM-Series Deployment Guide
- Create the init-cfg.txt File - VM-Series Deployment Guide
- Prepare the Bootstrap Package - VM-Series Deployment Guide
- Panorama Administrative Roles - Panorama Administrator's Guide

Knowledge Base Articles

- How to Authorize and Install VM-Series Auth Codes - Knowledge Base

  ** Valid support credentials required*

Videos

- VM-Series Deployment: Bootstrapping Basics - YouTube

  ** While this video refers to AWS/Azure/GCP, it is applicable to deploying on Nutanix as well*

Technical Details

Nutanix

- Nutanix REST API - Overview
- Nutanix Developer Portal
- How to create service chain using REST API

Nutanix API Calls

Get List of Existing Clusters

```
https://{{host}}:9440/api/nutanix/v3/clusters/list
```

Create a New Network Function Chain

```
https://{{host}}:9440/api/nutanix/v3/network_function_chains
```

Get a List of Existing Network Function Chains

```
https://{{host}}:9440/api/nutanix/v3/network_function_chains/list
```

Palo Alto Networks

- PAN-OS® and Panorama™ API Guide

PAN-OS and Panorama API Calls

Generate API Key

```
https://{{host}}/api?type=keygen&user=admin&password=admin
```

Configure Devices

```
https://{{host}}/api/?type=config&action=get&xpath=/config/devices
```

Create Panorama Device Group

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name
='@@{Panorama_DeviceGroup}@@'
```

Create Panorama Template

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']
```

Create Template Stack

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template-stack/entry[@na
me='@@{Panorama_TemplateStack}@@']
```

Configure Network Interfaces via Template

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']/config/devices/entry[@name='localhost.localdomain']/network/interface
/ethernet/entry
```

Create Virtual Wire

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/network/virtual-wire/ent
ry[@name='@@{Panorama_Vwire}@@']
```

Create Security Zone

```
https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name=
'vsys1']/zone/entry[@name='@@{Panorama_Zone}@@']
```

Add Template Variable

```
https://{{host}}/api?key={{key}}&type=config&action=set&xpath=/config/devices/entry[@name='lo
calhost.localdomain']/vsys/entry[@name='vsys1']
```

Commit Changes

```
https://{{host}}/api?key={{key}}&type=commit&cmd=<commit></commit>
```

Activate Licenses

```
https://api.paloaltonetworks.com/api/license/activate?uuid={{uuid}}&cpuid={{cpuid}}&authCode=
{{authcode}}&serialNumber={{serialnumber}}
```

Show Device Licenses

```
https://{{host}}/api?key={{key}}&type=op&cmd=<request><batch><license><info></info></license>
</batch></request>
```